ON THE CONVERGENCE OF ALGEBRAIC CONTINUED FRACTIONS WHOSE COEFFICIENTS HAVE LIMITING VALUES*

BY

EDWARD B. VAN VLECK

PADÉ† has shown that a power series $P(z)$ gives rise ordinarily to three types of regular continued fractions having the forms:

$$\text{(I)} \qquad \frac{U_0(z)}{V_0(z)} + \frac{a_2 z^{p_2}}{1} + \frac{a_3 z}{1} + \frac{a_4 z}{1} + \frac{a_5 z}{1} + \cdots,$$

$$\text{(II)}‡ \qquad \frac{U_1(z)}{V_1(z)} + \frac{b_2 z^{p_2}}{c_2 z + d_2} + \frac{b_3 z^2}{c_3 z + d_3} + \frac{b_4 z^2}{c_4 z + d_4} + \frac{b_5 z^2}{c_5 z + d_5} + \cdots,$$

$$\text{(III)} \qquad \frac{U_2(z)}{V_2(z)} + \frac{e_2 z^{p_2}}{f_2 z + g_2} + \frac{e_3 z}{f_3 z + g_3} + \frac{e_4 z}{f_4 z + g_4} + \frac{e_5 z}{f_5 z + g_5} + \cdots,$$

in which $U_i(z)$, $V_i(z)$ denote certain polynomials with which we need not concern ourselves here. The object of the following note is to investigate the convergence of these three classes of continued fractions upon the hypothesis that the coefficients $a_n, b_n, \cdots, g_n$ have limiting values for $n = \infty$. The results obtained below for the first two types of continued fractions are in no wise dependent upon the value of p_2 nor upon the nature of the polynomials U_i, V_i, neither are they affected by the introduction of a finite number of irregularities into the continued fraction—that is to say, by the presence of a finite number of partial numerators or denominators of degree higher than the normal. This is not true of the third type of continued fractions.

§ 1. *Preliminary discussion for type* I.

Consider first a continued fraction of this type which is regular from the beginning. The result which will be proved is as follows:

* Presented to the Society February 27, 1904. Received for publication April 26, 1904.

† *Thesis*, Annales de l' Ecole Normale, ser. 3, vol. 9, supplement (1892).

‡ If $1/x$ be substituted for z, type II appears in the familiar form:

$$\frac{U(x)}{V(x)} + \frac{b_2}{d_2 x + c_2} + \frac{b_3}{d_3 x + c_3} + \cdots.$$

THEOREM. *If in the continued fraction*

$$A(z) = \frac{1}{1} + \frac{a_2 z}{1} + \frac{a_3 z}{1} + \cdots, \tag{1}$$

lim $a_n = k$ *for* $n = \infty$, *the continued fraction will converge over the entire plane of* z *except* (1) *along the whole or a part of a rectilinear cut drawn from* $z = -1/4k$ *to* $z = \infty$ *with an argument equal to that of the vector from the origin to* $z = -1/4k$, *and except possibly*, (2) *at certain isolated points* $p_1, p_2, p_3, \cdots$. *Within the plane so cut the limit of the continued fraction is holomorphic except at the points* $p_1, p_2, p_3, \cdots$, *which are poles.*

This result I have previously established under certain restrictions in the Annals of Mathematics,* and application was there made to the continued fractions of GAUSS, HEINE and BESSEL. To remove these restrictions a new and simpler method of proof is adopted here.

The proof is founded upon the familiar formula:

$$A(z) = \frac{N_n}{D_n} + (-)^n a_2 a_3 \cdots a_n z^{n-1} \left(\frac{a_{n+1} z}{D_n D_{n+1}} - \frac{a_{n+1} a_{n+2} z^2}{D_{n+1} D_{n+2}} + \frac{a_{n+1} a_{n+2} a_{n+3} z^3}{D_{n+2} D_{n+3}} - \cdots \right), \tag{2}$$

in which N_n and D_n denote the numerator and denominator of the nth convergent of (1). Between three consecutive denominators their exists the relation

$$D_{n+1} = D_n + a_{n+1} z D_{n-1}, \tag{3}$$

which by hypothesis has the limiting form

$$D_{n+1} - D_n - kz D_{n-1} = 0.$$

Now POINCARÉ† has shown that when a limiting form exists for the recurrent relation and the roots of the auxiliary equation

$$x^2 - x - kz = 0 \tag{4}$$

are of unequal modulus, the quotient D_{n+1}/D_n will converge to a limit which is the one or the other of the roots of (4). Since these roots are

$$x = \tfrac{1}{2} \pm \sqrt{\tfrac{1}{4} + kz},$$

their moduli will be equal only when $kz + \frac{1}{4}$ is a negative number, that is, when $|z| > 1/4|k|$ and z has the same argument as $-1/k$.

* Ser. 2, vol. 3 (1901), p. 13.

† American Journal of Mathematics, vol. 7 (1885), p. 213. POINCARÉ's theorem is cited for the special case of a recurrent relation of the 2d order.

We shall exclude such values of z by drawing the cut already described in the theorem. Then at any point not on the cut we have

$$\lim_{n=\infty} \frac{D_{n+1}}{D_n} = \beta, \tag{5}$$

in which β is a root of (4), and the ratio of the rth term of (2) to the preceding has the limit $-kz/\beta^2$. Since $-kz$ is the product of the roots of (4), the absolute value of this ratio will be less than 1 if β is the root which has the larger modulus, while it will be greater than 1 if β is the other root. Furthermore, it is clear from (5) that n can be taken so large that no one of the denominators on the right hand side of (2) will vanish at an assigned point z, not lying upon the cut. Hence the continued fraction will converge outside the cut at every point for which β is the root of (4) which has the greater modulus, while it increases indefinitely at the remaining points.*

§ 2. *Proof of Poincaré's Theorem.*

It will be necessary to show next that the last mentioned points can condense in infinite number only in the vicinity of a point upon the cut. With this ultimate object in view, it will be desirable to give here a new and simple proof of POINCARÉ's theorem. Let β', β'' denote the two roots of (4) or, more generally, of the auxiliary quadratic for *any* recurrent relation of the 2d order with a limiting form. If a sufficiently large value of n is taken, the recurrent relation can be expressed in the form

$$(D_{n+1} - \beta' D_n) - (\beta'' + \bar{\epsilon}_{n+1})(D_n - \beta' D_{n-1}) + \bar{\epsilon}'_{n+1} D_{n-1} = 0,$$

in which $|\bar{\epsilon}_{n+1}|$ and $|\bar{\epsilon}'_{n+1}|$ are smaller than a small positive quantity, arbitrarily prescribed. The last equation may be written

$$(D_{n+1} - \beta' D_n) - (\beta'' + \epsilon''_{n+1})(D_n - \beta' D_{n-1}) = 0, \tag{6}$$

where

$$\epsilon''_{n+1} = \bar{\epsilon}_{n+1} - \frac{\bar{\epsilon}'_{n+1} D_{n-1}}{D_n - \beta' D_{n-1}}.$$

Consequently, if there is any set of values of n, infinite it number, for which the point $\rho_n = D_n/D_{n-1}$ does not come at least once within less than an assigned distance of β', we may make $|\epsilon''_{n+1}|$ smaller than any given quantity ϵ by increasing n within the set. Similarly we have

$$D_{n+1} - \beta'' D_n = (\beta' + \epsilon'_{n+1})(D_n - \beta'' D_{n-1}) \qquad (|\epsilon'_{n+1}| < \epsilon), \tag{7}$$

* Thus far the work has been identical with that of PINCHERLE in his consideration of continued fractions of type II. Cf. Annales de l'Ecole Normale, ser. 3, vol. 6 (1889), p. 144; also Giornale di Matematiche, vol. 32 (1894), p. 234–6. PINCHERLE, however, goes no further and does not settle the character of the point set for which β is the smaller root of (4). In consequence, his result is an indefinite one, and he misses the theorems of the present paper.

for a sufficiently large n in any set of values for which ρ_n lies without some assigned distance of β''. The last equation may be written

$$\rho_{n+1} - \beta'' = \frac{\beta' + \epsilon'_{n+1}}{\rho_n}(\rho_n - \beta''), \tag{8}$$

and its division by (6) gives

$$\frac{\rho_{n+1} - \beta''}{\rho_{n+1} - \beta'} = \frac{\beta' + \epsilon'_{n+1}}{\beta'' + \epsilon''_{n+1}} \cdot \frac{\rho_n - \beta''}{\rho_n - \beta'} \quad (|\epsilon'_{n+1}| < \epsilon, |\epsilon''_{n+1}| < \epsilon). \tag{9}$$

Equation (9) holds for a sufficiently large value of n provided ρ_n lies without an arbitrarily small but prescribed distance of β' and β'', as I shall for a time assume. Denote this distance by d and consider the circle $|\rho - \beta''| = d$. By taking d sufficiently small, the ratio of the maximum to the minimum of

$$\left|\frac{\rho - \beta''}{\rho - \beta'}\right|$$

for points upon this circle can be made as nearly equal to 1 as we please. Let this ratio be $1 + \epsilon'$, in which ϵ' is taken small enough to fulfill the inequality which is given just below.

Suppose now that $|\beta'| > |\beta''|$. Then it is clear from (9) that upon increasing n by 1, the quotient $|\rho_n - \beta''| / |\rho_n - \beta'|$ is increased by a factor at least as great as the quantity

$$\frac{|\beta'| - \epsilon}{|\beta''| + \epsilon} > |1 + \epsilon'| > 1.$$

Hence as ρ_n, by hypothesis, lies without the circle, ρ_{n+1} does also. But when (9) holds for a series of successive values of n, we get a set of points $\rho_n, \rho_{n+1}, \rho_{n+2}, \cdots$, gravitating toward β' as a limit, and this continues until (9) breaks down. The last will not happen until ρ_{n+m} falls within circle $|\rho - \beta'| = d$. But then $\rho_{n+m+1} - \beta''$ and $\rho_{n+m} - \beta''$, by (8), are nearly identical vectors since ρ_{n+m} differs but little from β'. Hence the first of the points ρ_{n+m+1} $(i = 1, 2, \cdots)$ which falls without the circle $|\rho - \beta'| = d$ will differ infinitesimally from $\rho_{n+m+i-1}$ which lies within. As soon, however, as ρ_{n+m+i} falls without the circle, equation (9) operates immediately to draw it back again into the interior. If, finally, d be made smaller and smaller, it follows that the distance $\rho_n - \beta'$ becomes and remains eventually as small as we wish. Thus we conclude that unless ρ_n, from and after some fixed value of n, remains within an arbitrarily assigned distance of β'', it must approach β' as its limit. In other words, one of the two values β', β'' is its limit, as was to be proved.

§ 3. *Completion of discussion for type* I.

We return now to the continued fraction (1) and give to z a fixed value not on the cut. If a sufficient number of terms of (1) are omitted at the outset, a new continued fraction will be obtained,

$$A_m(z) = \frac{a_{m+1}z}{1} + \frac{a_{m+2}z}{1} + \frac{a_{m+3}z}{1} + \cdots, \tag{10}$$

in which all the partial numerators differ from their limit kz by as little as we please. For this continued fraction

$$D_0 = D_1 = 1, \qquad \rho_1 = \frac{D_1}{D_0} = 1.$$

Now the auxiliary equation has a root equal to 1 only if $k = 0$. Suppose first $k \neq 0$ and apply the reasoning of § 2 to (10), taking ϵ and d to be extremely small. Then

$$|\rho_1 - \beta''| > d, \qquad |\rho_1 - \beta'| > d.$$

Hence equation (9) takes effect at the very beginning of the continued fraction, and we obtain a sequence of points $\rho_1, \rho_2, \rho_3, \cdots$, approaching β' as a limit. For the particular case in which $k = 0$, we have $\beta' = 1$, and this root is *a fortiori* the limit of $\rho_n = D_n / D_{n-1}$. We conclude therefore in either case that the limit of ρ_n is that root of (4) which has the greater modulus, and consequently the continued fraction (10) will converge at the assigned point z, provided, of course, the value of m is taken sufficiently large.

The same argument holds simultaneously for values of z in the immediate vicinity of the chosen point. Take then a very small circle C enclosing the point. For this circle $|z|$ will have an upper limit U and $|\beta'|$ a lower limit L. Hence from and after some fixed value of n the series (2)—when constructed for the continued fraction (10)—will be comparable with a geometric progression in which the ratio of each term to the preceding is

$$\frac{kU(1+\epsilon)}{L^2(1-\epsilon)} < 1.$$

Hence the convergence of the series is uniform in this circle, and from this fact the analytic character of its limit immediately follows.

Let the nth convergent of (10) be denoted now by N'_n/D'_n. Then the $(n+m)$th convergent of (1) is

$$\frac{N_m + \dfrac{N'_n}{D'_n} N_{m-1}}{D_m + \dfrac{N'_n}{D'_n} D_{m-1}}.$$

Since N'_n/D'_n within the circle C has a limit $A_m(z)$, the continued fraction (1) must likewise converge to a limit

$$\frac{N_m + A_m(z) N_{m-1}}{D_m + A_m(z) D_{m-1}}, \tag{11}$$

except at the points of the circle C in which the denominator of (11) vanishes. If it should vanish identically, then $-D_m/D_{m-1}$ and $A_m(z)$ have the same expansion into a continued fraction. But this is impossible, since $A_m(z)$, by hypothesis, has an expansion (10) containing an infinite number of terms, whereas the development of a rational fraction D_m/D_{m-1} in a continued fraction of the form (10), as is well known, has only a limited number of terms. Accordingly the denominator of (11) is not 0 but an analytic function. Since the zeros of such a function are isolated, it follows that the continued fraction (1) is either holomorphic or meromorphic within the circle C. Now for the center of C any point not upon the cut can be chosen. Our conclusion therefore can be extended to the entire plane exterior to the cut. Thus the theorem stated at the beginning of § 1 is established.

The reasoning is not affected in any way if a finite number of partial numerators or denominators in (1) are replaced by polynomials.

§ 4. *The second class of continued fractions.*

The investigation of the second type of continued fractions when limiting values exist for the coefficients can be reduced quickly to the previous investigation for type I. To this end let (II) be written

$$(12)\qquad \frac{U_1(z)}{V_1(z)}+\cfrac{b_2z^{p_2}}{c_2z+d_2}\Bigg/1+\cfrac{b_3z^2}{(c_2z+d_2)(c_3z+d_3)}\Bigg/1+\cfrac{b_4z^2}{(c_3z+d_3)(c_4z+d_4)}\Bigg/1+\cdots.$$

Then make the substitution

$$(13)\qquad x=\frac{\sqrt{b}\,z}{cz+d}$$

in which b, c, d denote the limits of b_n, c_n, d_n $(n=\infty)$. Choose for x any fixed point of the finite plane or any value in its immediate vicinity. If enough partial fractions at the beginning of (12) are omitted, the remainder of the continued fraction may be written

$$(14)\qquad \cfrac{x^2(1+\epsilon_{m+1})}{1}+\cfrac{x^2(1+\epsilon_{m+2})}{1}+\cdots,$$

where $\epsilon_{m+1}, \epsilon_{m+2}, \cdots$ are rational functions of x, the absolute values of which will be less than a given positive number ϵ for a sufficiently small neighborhood about the fixed point.

The application of § 3 to the continued fraction (14) shows then that it converges uniformly in such a neighborhood, provided ϵ is small enough and the fixed point does not lie upon a cut along the imaginary axis of the x-plane exterior to the points $x^2=-\frac{1}{4}$. To this cut there corresponds by (13) a cut

along an arc of a circle in the z-plane, and to the fixed x-point there corresponds a z-point exterior to the cut. Returning now to the continued fraction (12) or (II), we conclude that it will converge uniformly in the vicinity of the z-point when a sufficient number of terms is omitted. Let $A_m(z)$ denote the limit after the omission in (II). Then for the $(n+m)$th convergent of (II) we have again such an expression as (11). But D_n/D_{n-1} when expanded into a continued fraction of type II, has only a finite number of terms,* whereas $A_m(z)$ has an infinite number. Consequently $D_m + D_{m-1}A_m(z)$ can not vanish identically. The following theorem therefore results:

If in the continued fraction (II)

$$\lim b_n = b, \qquad \lim c_n = c, \qquad \lim d_n = d,$$

it will converge over the entire plane of z except (1) *at isolated points and* (2) *upon the whole or a part of a cut along the arc of a circle into which the segments of the imaginary axis of x exterior to the points $x^2 = -\frac{1}{4}$ are converted by the transformation* (13). *In the plane thus cut the limit of the continued fraction is holomorphic except at these isolated points which are poles.*

If the alternate convergents of (I) are formed into two distinct sets, those of either set are by themselves the successive convergents of a continued fraction of type II, in which the partial fractions after the opening irregularity have the form

$$\frac{-a_{n-1}a_n z^2}{1 + a_{n+1}z + a_n z}.$$

It is easy to see that this expression has the same limiting form for odd and for even values of n if, and only if, a_{2n} and a_{2n+1} have limits. That then the analytic functions which are limits of the two sets of convergents are identical follows at once from a theorem which I have given in a previous paper.†

Thus when a_{2n} and a_{2n+1} in (I) *have separate limits, a theorem holds similar to that previously given except that the cut is in general the arc of a circle.*

§ 5. *Restrictions on the power-series.*

The relations between the coefficients of the continued fraction and of the corresponding power-series

$$P(x) = l_0 - l_1 z + l_2 z^2 - l_3 z^3 + \cdots$$

* This can be made clear to the reader who is familiar with PADÉ's thesis in the following manner: Let PADÉ's table be formed for the power series $P(x)$ which is the development of a rational fraction $N'_{p'}/D'_{q'}$ with numerator and denominator of the p'th and q'th degrees respectively. His approximants U_p/V_q will be identical with $N'_{p'}/D'_{q'}$, for $p \geqq p'$, $q \geqq q'$. Now to a continued fraction of type II there corresponds in PADÉ's table a diagonal line of approximants, which from and after some fixed element of the line are identical with $N'_{p'}/D'_{q'}$. In other words, the continued fraction terminates.

† Transactions, vol. 2 (1901), p. 476.

have been given by FROBENIUS.* In case the continued fraction (1) is regular from the beginning we put†

$$A_n = \begin{vmatrix} l_0 & l_1 & \cdots & l_{n-1} \\ l_1 & l_2 & \cdots & l_n \\ \cdots & \cdots & \cdots & \cdots \\ l_{n-1} & l_n & \cdots & l_{2n-2} \end{vmatrix}, \qquad B_n = \begin{vmatrix} l_1 & l_2 & \cdots & l_n \\ l_2 & l_3 & \cdots & l_{n+1} \\ \cdots & \cdots & \cdots & \cdots \\ l_n & l_{n+1} & \cdots & l_{2n-1} \end{vmatrix},$$

also

$$m_{2n} = \frac{A_n^2}{B_{n-1}B_n}, \qquad m_{2n+1} = \frac{B_n^2}{A_nA_{n+1}}.$$

Then we have

$$a_n = \frac{1}{m_{n-1}m_n}$$

or

$$a_{2n} = \frac{A_{n-1}B_n}{A_nB_{n-1}}, \qquad a_{2n+1} = \frac{A_{n+1}B_{n-1}}{A_nB_n}. \tag{15}$$

Suppose now that

$$\lim a_{2n} = a', \qquad \lim a_{2n+1} = a''. \tag{16}$$

Then

$$\lim_{n=\infty} \sqrt[n]{a_1a_2a_3\cdots a_{2n-1}} = \lim \sqrt[n]{\frac{A_n}{A_{n-1}}} = a'a'',$$

$$\lim_{n=\infty} \sqrt[n]{a_1a_2a_3\cdots a_{2n}} = \lim \sqrt[n]{\frac{B_n}{B_{n-1}}} = a'a''.$$

Let us place

$$\frac{A_n}{A_{n-1}} = (a'a'')^n q_n', \qquad \frac{B_n}{B_{n-1}} = (a'a'')^n q_n'',$$

and substitute in (15), finally in (16). In this manner we find that *the series will generate a regular continued fraction* (1) *with limits for* a_{2n} *and* a_{2n+1}‡ *when, and only when, the following conditions are fulfilled*: §

(1) $A_n \neq 0$, $B_n \neq 0$ *for all values of* n.§

*Journal für Mathematik, vol. 90 (1881), p. 5.

†See also the memoir of STIELTJES, Annales de la Faculté des Sciences de Toulouse, vol. 8 (1894), J, pp. 26 and 3.

‡The conditions for the existence of other continued fractions of type I, which, though not regular throughout, possess a like property can be expressed similarly with the aid of the determinants $c_{\alpha\beta}$ of FROBENIUS. The continued fraction (1) which was selected above, corresponds to a step-like line of approximants starting from the corner of PADÉ's table, and is used much more than the remaining continued fractions of type I.

§If $A_n = 0$ and $B_n = 0$ for only a finite number of values of n, irregularities will occur for a time in the continued fraction, but limits for a_{2n} and a_{2n+1} will still exist, if the other two conditions are satisfied.

(2) *A common limit a exists for* $\sqrt[n]{A_n/A_{n-1}}$ *and* $\sqrt[n]{B_n/B_{n-1}}$.

(3) *Limits also exist for* q_n'/q_{n-1}'' *and* q_n''/q_n' *in which*

$$q_n' = \frac{A_n}{a^n A_{n-1}}, \qquad q_n'' = \frac{B_n}{a^n B_{n-1}}.$$

§ 6. *The third class of continued fractions.*

A parallel discussion of (III) leads to somewhat different results. Let it be expressed in the form

$$\frac{U_2}{V_2} + \cfrac{e_2 z^{p_2}}{f_2 z + g_2} + \cfrac{e_3 z}{(f_3 z + g_3)(f_2 z + g_2)} + \cfrac{e_4 z}{(f_4 z + g_4)(f_3 z + g_3)} \cdots,$$

and then put

$$x' = x^2 = \frac{ez}{(fz + g)^2}, \tag{17}$$

in which e, f, g denote the limits of e_n, f_n, g_n. We obtain such a continued fraction as (14).* A difference, however, manifests itself in passing thence to the equation of the form (11) which gives the $(n+m)$th convergent of (III). For it is not the case that the expansion of a rational fraction into a continued fraction of the third type will have necessarily only a finite number of terms. Consequently it is possible for the denominator of (11) to vanish identically, and the convergence or divergence of our continued fraction will depend upon its initial terms or upon any irregularities which may be introduced. Take, for example, the continued fraction

$$\frac{U_2(z)}{U_3(z)} - \cfrac{z}{1+z} - \cfrac{z}{1+z} - \cfrac{z}{1+z} - \cdots.$$

If the first partial fraction be omitted, the nth convergent is

$$-z\frac{1 + z + \cdots + z^{n-1}}{1 + z + z^2 + \cdots + z^n},$$

which has the limit $-z$ if $|z| < 1$ and the limit -1 if $|z| > 1$. Hence the original continued fraction diverges for $|z| < 1$ if $U_3(z) = z$ and for $|z| > 1$ if $U_3(z) = 1$.

The form of cut to be made in limiting the region of convergence can be found by transforming the rectilinear cut for (14) by the substitution (17). This substitution, by a linear change in the x'- and z-coördinates, can be reduced to

$$x' = \tfrac{1}{2}\left(z' + \frac{1}{z'}\right),$$

* e_{m+n} and the convergents are still rational in z, though not in x.

which is discussed thoroughly in HOLZMÜLLER'S *Theorie der isogonalen Verwandschaften*, p. 143.

Attention should be called to one special case of frequent occurrence. Place first $g = 1$, which may be done without loss of generality. Then suppose $e = -f$. Equation (17) may be written

$$\tfrac{1}{2}\left(\frac{1}{x'} + 2\right) = \tfrac{1}{2}\left(ez + \frac{1}{ez}\right),$$

By this substitution the rectilinear cut along the real axis of the x-plane from $x' = -\frac{1}{4}$ to $x' = -\infty$ is converted into the entire circumference of a circle of the z-plane having the origin as its center and having a radius equal to $1/e$. The region of convergence is therefore in this case a circle.

WESLEYAN UNIVERSITY,
MIDDLETOWN, CONN.

THE SYLOW SUBGROUPS OF THE SYMMETRIC GROUP*

BY

WILLIAM FINDLAY

In the Sylow theorems† we learn that if the order of a group $\mathfrak{A}$ is divisible by p^α (p a prime integer) and not by $p^{\alpha+1}$, then $\mathfrak{A}$ contains one and only one set of conjugate subgroups of order p^α, and any subgroup of $\mathfrak{A}$ whose order is a power of p is a subgroup of some member of this set of conjugate subgroups of $\mathfrak{A}$. These conjugate subgroups may be called the Sylow subgroups of $\mathfrak{A}$. It will be our purpose to investigate the Sylow subgroups of the symmetric group of substitutions.

By means of a preliminary lemma the discussion will be reduced to the case where the degree of the symmetric group is a power (p^α) of the prime (p) under consideration.

A set of generators of the group having been obtained, they are found to set forth, in the notation suggested by their origin, the complete imprimitivity of the group. The various groups of substitutions upon the systems of imprimitivity, induced by the substitutions of the original group, are seen to be themselves Sylow subgroups of symmetric groups of degrees the various powers of p less than p^α. They are also the quotient groups under the initial group of an important series of invariant subgroups.

In terms of the given notation convenient exhibitions are obtained of the commutator series of subgroups and also of all subgroups which may be considered as the Sylow subgroups of symmetric groups of degree a power of p.

Enumerations are made of the substitutions of periods p and p^α and the conjugacy relations of the latter set of substitutions are discussed.

The subgroup consisting of all substitutions invariant under the main group is cyclic and of order p.

The full set of conjugate Sylow subgroups of the symmetric group on p^α letters fall into

$$\frac{p^\alpha!}{(p!)^\alpha} \qquad (\alpha = p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1)$$

classes each consisting of $\{(p-2)!\}^\alpha$ groups having the same complete system of imprimitivity.

* Presented to the Society February 27, 1904. Received for publication June 20, 1903.

† Mathematische Annalen, vol. 5 (1873), page 584.

§ 1. *Lemma.*

We define the function $\pi(n, p)$ of p any prime and n any integer, as the exponent of the highest power of p occurring as a factor of $n!$. If we impose the restriction that no power of p shall occur in the summation more than $p-1$ times, n is uniquely expressible in the form

$$n = \sum_{i=1}^{k} p^{a_i}, \qquad a_i \geqq 0.$$

We have the relation*

$$\pi(n, p) = \frac{n-k}{p-1}.$$

In particular

$$\pi(p^a, p) = \frac{p^a - 1}{p-1},$$

and therefore

$$\pi(n, p) = \sum_{i=1}^{k} \pi(p^{a_i}, p).$$

§ 2. *Reduction of the problem.*

Throughout this paper, German capitals will be used to denote groups and the corresponding Roman capitals to represent substitutions; thus, $\mathfrak{A}_\alpha^a$ represents a group of degree a and order α and its substitutions will in general be denoted by $A_1, A_2, \cdots$. The symmetric group of degree n will be denoted by $\mathfrak{S}^n$ and its Sylow subgroup of order a power of p, by $\mathfrak{P}^n$. The letter E, with suffixes, will be used for the elements of $\mathfrak{P}$ which are considered as its generators. Our main problem is to find one subgroup $\mathfrak{P}^n$ of $\mathfrak{S}_{n!}^n$ having order $p^{\pi(n,p)}$.

If $a < c$, any substitution, or group of substitutions on a letters — we will speak of the objects upon which the substitution is performed as *letters* — may properly be considered as an element or subgroup of $\mathfrak{S}^c$.

Given a number of groups

$$\mathfrak{A}_\alpha^a, \mathfrak{B}_\beta^b, \cdots, \mathfrak{K}_\kappa^k,$$

if we consider the letters of the different groups as wholly distinct and the groups as subgroups of $\mathfrak{S}^m$, $m = a + b + \cdots + k$, then their least common overgroup consists of the totality of products of the form

$$A \cdot B \cdots K$$

and its order is $\alpha \cdot \beta \cdots \kappa$.

By the lemma of § 1, we can find a set of powers of p, say

$$p^{a_1}, p^{a_2}, \cdots, p^{a_r},$$

such that

1) $$n = \sum_{i=1}^{r} p^{a_i},$$

* BACHMANN, *Zahlentheorie*, I, p. 33.

2) $$\pi(n, p) = \sum_{i=1}^{r} \pi(p^{a_i}, p).$$

Distributing the n letters of $\mathfrak{S}^n$ into r sets containing $p^{a_1}, p^{a_2}, \cdots, p^{a_r}$ letters, respectively, we see that $\mathfrak{P}^n$ is the least common overgroup of a set of Sylow subgroups *

$$\mathfrak{P}^{p^a} \qquad (i=1, 2, 3, \cdots, r).$$

Since it is also a subgroup of $\mathfrak{P}^{p^a}$, $p^a > n$, it may be considered sufficient to investigate only the case where n is a power of p.

§ 3. *Generation of a* $\mathfrak{P}^{p^a}_{p^{\pi(p^a, p)}}$. †

We shall obtain $\mathfrak{P}^{p^a}$ by an inductive process, assuming the knowledge of a $\mathfrak{P}^{p^{a-1}}$. Distribute the p^a letters into p corresponding sets each containing p^{a-1} letters. This we may indicate by the notation for the letters

$$\mathrm{L}_{i,j} \qquad (i=1, 2, \cdots, p; j=1, 2, 3, \cdots, p^{a-1}).$$

Let $\mathfrak{A}'$ be a $\mathfrak{P}^{p^{a-1}}$ on the letters $\mathrm{L}_{1,j}$. Transforming this by the p substitutions

$$\mathrm{S}_i = \begin{pmatrix} \mathrm{L}_{1,1}, & \mathrm{L}_{1,2}, & \cdots, & \mathrm{L}_{1,p^{a-1}} \\ \mathrm{L}_{i,1}, & \mathrm{L}_{i,2}, & \cdots, & \mathrm{L}_{i,p^{a-1}} \end{pmatrix} \qquad (i=1, 2, \cdots, p),$$

we obtain a series of groups $\mathfrak{A}'$, $\mathfrak{A}''$, $\mathfrak{A}''' \cdots \mathfrak{A}^{(p)}$, whose least common overgroup $\mathfrak{Q}$ (§ 2) is of degree p^a and order

$$p^{p \cdot \pi(p^{a-1}, p)}.$$

Now

$$\pi(p^{a-1}, p) = p^{a-2} + p^{a-3} + \cdots + p + 1.$$

Therefore the degree of $\mathfrak{Q}$ is

$$p^{\pi(p^a, p)-1}.$$

The substitution

$$\mathrm{E} = \begin{pmatrix} \cdots & \mathrm{L}_{i,j} & \cdots \\ & \mathrm{L}_{h,j} & \end{pmatrix},$$

where $h \equiv i+1$, mod. p, $1 \leqq h \leqq p$, $i = 1, 2, 3, \cdots, p$, has the following properties:

1) $$\mathrm{E}^{-1}\mathrm{A}^{(i)}\mathrm{E} = \mathrm{A}^{(h)}.$$

Therefore the product of two substitutions of the form

$$\mathrm{QE}^k$$

may again be expressed in the same form.

* Cf. G. A. MILLER, *On the Transitive Substitution Groups whose order is a power of a Prime Number*, American Journal of Mathematics, vol. 23 (1901), p. 176.

† Cf. NETTO, *Theory of substitutions* (translated by COLE), § 39, page 41.

2) If Q changes L_{ij} into $L_{i,g}$, then QE^k will change L_{ij} to $L_{h,g}$ where $h \equiv i + k$, mod. p. Therefore

$$QE^k = Q'E^{k'}$$

if, and only if, $Q = Q'$ and $k \equiv k$, mod. p.

Hence it follows that the totality of substitutions of the form QE^k constitute a group of order

$$p^{\pi(p^a, p)},$$

which is therefore a $\mathfrak{P}^{p^a}$.

The process of induction obtained above is to be conceived of as beginning with $a = 1$. The Q in this case is the identity substitution. For the full application of the induction it is required that the original p^a letters be distributed into p sets, which we shall call the subsets of order one, then each of these into p subsets of order two, each of the latter subsets into p subsets of order three, and so on until finally we have the subsets of order a consisting of one letter each. The required correspondence between the letters in the p subsets of order $h + 1$ into which any subset of order h is divided is to be obtained by ordering the p subdivisions at each stage. For convenience the totality of the p^a letters will be spoken of as the subset of order 0.

All these requirements are met by the following a-partite suffix notation:

$$L_{\{b_1, b_2, \cdots, b_a\}},$$

where $1 \leqq b_i \leqq p$ $(i = 1, 2, \cdots, a)$.

The first g elements in the suffix define the subset of order g to which the letter belongs, the $(g+1)$th suffix which of the p subsets of this division contains it and the remaining $a - g - 1$ elements serve to establish the required correspondence of these p subsets of order $g + 1$. Here g has the range $g = 0, 1, 2, \cdots, a - 1$.

The E required to obtain a particular $\mathfrak{P}^{p^{a-g}}$ $(0 \leqq g \leqq a - 1)$, (say that which acts upon the subset of order g whose letters have $c_1, c_2, \cdots, c_g$ as the first g elements in their suffix), from the $p\mathfrak{P}^{p^{a-g-1}}$ upon the p subsets of order $g + 1$ contained in the above, will be

$$E_{\gamma_g} \equiv E_{\{c_1, c_2, \cdots, c_g\}} \equiv \begin{pmatrix} \cdots, & L_{\{b_1, b_2, \cdots, b_a\}}, & \cdots \\ & L_{\{d_1, d_2, \cdots, d_a\}} & \end{pmatrix},$$

where

$$d_{g+1} \equiv b_{g+1} + 1 \,(\text{mod. } p) \text{ if } b_i = c_i \; (i = 1, 2, \cdots, g),$$

$$d_{g+1} = b_{g+1}, \text{ if for some } i, \text{ in } i = 1, 2, \cdots, g, \; b_i \neq c_i,$$

$$d_j = b_j \qquad (j = 1, 2, \cdots, g, g+2, \cdots, a).$$

Hereafter we shall use α_g, β_g, γ_g, etc., as symbols for g-partite numbers with elements a_i, b_i, c_i, etc. The general g-partite number with elements having range $1, 2, 3, \cdots, p$ will be denoted by $\lambda_g \equiv \{l_1, l_2, \cdots, l_g\}$ and the totality

of these, p^g in number, will be denoted by Λ_g. For $g=0$ we have but one E which we may denote by E_0.

The totality of E_{λ_g}'s ($g=0, 1, \cdots, a-1$), in number

$$\pi(p^a, p) = \sum_{g=0}^{a-1} p^g,$$

constitute a system of generators of a $\mathfrak{P}^{p^a}$.

§ 4. *A normal form for the general* P.

We shall say that λ_g is contained in λ'_h if 1) $g<h$, 2) $l_i = l'_i$ ($i=1, 2, \cdots, g$). If λ_g and λ'_h are not the same and neither one contains the other they will be said to be independent.

From the expression for the E's in § 3, it is seen that if λ_g is contained in λ_h, then

$$E^{-1}_{\lambda_g} E_{\lambda_h} E_{\lambda_g} = E_{\lambda'_h},$$

where

$$l'_{g+1} \equiv l_{g+1} + 1 \pmod{p},$$
$$l'_i = l_i \qquad (i=1, 2, \cdots, g, g+2, \cdots, h),$$

and that if λ_g and λ'_h are independent,

$$E^{-1}_{\lambda_g} E_{\lambda'_h} E_{\lambda_g} = E_{\lambda'_h}.$$

These results may be generalized and stated in the following form:

a) If λ_g is contained in λ_h, then

$$E^b_{\lambda_h} \cdot E^c_{\lambda_g} = E^c_{\lambda_g} \cdot E^b_{\lambda'_h},$$

where

$$l'_{g+1} \equiv l_{g+1} + c \pmod{p},$$
$$l'_i = l_i \qquad (i=1, 2, \cdots, g, g+2, \cdots, h).$$

b) If λ_g and λ'_g are independent, then

$$E^b_{\lambda_g} \cdot E^{c'}_{\lambda'_h} = E^{c'}_{\lambda'_h} \cdot E^b_{\lambda_g}.$$

By means of these formulas any product of the E's, that is, any substitution of $\mathfrak{P}^{p^a}$, can be expressed in the form

$$P = \prod_{g=0, 1, 2, \cdots, a-1} \prod_{\lambda_g | \Lambda_g} E^{k_{\lambda_g}}_{\lambda_g},$$

where $0 \leqq k_{\lambda_g} \leqq p-1$, and the symbol $\lambda_g | \Lambda_g$ indicate that λ_g takes all values in Λ_g. The arrangement of the terms in the inner product is immaterial since they are commutative with each other.

This we shall call the normal form of P in terms of the generators. The set of k's is uniquely determined.

§ 5. *Normal form* for* P^{p^a}.

It is desired to find the set of k''s such that

$$\mathrm{P}^{p^a} = \Pi\,\Pi \mathrm{E}_{\lambda_g}^{k'_{\lambda_g}}.$$

We shall conceive this normalized form to be obtained from the product of p^a factors each of which is P written in its normal form by assembling to the left first the E's with $g = 0$, next the E's with $g = 1$, then the E's with $g = 2$ and so on, making use of the formulas of § 4. Let

$$k_{\{l_{1,b},\, l_{2,b},\, \cdots,\, l_{g,b}\}} \qquad (1 \leqq b \leqq p^a)$$

be the exponent of E_{λ_g} in the bth factor of the product, numbering from the right, after all the E_{λ_h}, with $h < g$, have been assembled to the left. The exponents of the $(b+1)$th term differ from the corresponding ones in the bth term only in the effects produced by the parts of the bth term as they passed over. Therefore

$$l_{h+1,\,b+1} \equiv l_{h+1,\,b} - k_{\{l_{1,b},\, l_{2,b},\, \cdots,\, l_{h,b}\}} \pmod{p}.$$

Each $\mathrm{E}_{\lambda_g}^k$ is unaffected as it passes to the left, over the residues of terms, since the latter contain only $\mathrm{E}_{\lambda_h'}$ with $h \geqq g$. We have then

$$k'_{\lambda_g} \equiv \sum_{b=1}^{p^a} k_{\{l_{1,b},\, l_{2,b},\, \cdots,\, l_{g,b}\}} \pmod{p}.$$

§ 6. *The imprimitivity of* $\mathfrak{P}^{p^a}$.

The complex classification of the letters L_{λ_a} furnished by the a-partite suffix λ_a may be regarded as comprising $a-1$ simple classifications, viz., the distributions of the p^a letters into p^h subsets of order h, p^{a-h} in each subset $(h = 1, 2, \cdots, a-1)$.

THEOREM: Each of these simple classifications constitutes a division of the letters into sets of imprimitivity of the group.

This is equivalent to saying that, by a given substitution P, all letters having their first h suffixes the same in each will go into letters which agree in their first h suffixes.

The effect of P upon L_{λ_a} may be considered as produced by applying sucessively, beginning at the left, i. e., according to ascending values of g, the factors of the outer product in the normal form of P (§ 4). If P changes L_{λ_a} to L_{λ_a}' it will be seen that

1) The l_i''s are changed one by one and in order according to ascending values of i.

2) $$l'_{g+1} \equiv l_{g+1} + k'_{\lambda_g} \pmod{p} \qquad (g = 0, 1, 2, \cdots, a-1),$$

when λ_g' is contained in λ_a'.

* This normal form seems worthy of note although no use is made of it in the sequel.

Hence if L_{β_α} and L_{γ_α} have $b_i = c_i$ $(i = 1, 2, \cdots, h)$, then their transforms by P, $L_{\beta'_\alpha}$ and $L_{\gamma'_\alpha}$, have $b'_i = c'_i$ $(i = 1, 2, \cdots, h)$, which proves the theorem, and in addition that

$$b'_{h+1} - b_{h+1} \equiv c'_{h+1} - c_{h+1} \pmod{p}.$$

THEOREM: The analysis of the imprimitivity of $\mathfrak{P}$, given above, is complete, in the sense that it contains every subdivision of the letters into sets of imprimitivity of $\mathfrak{P}$.

For suppose we have a division of the p^a letters L_λ into p^a/n classes of n each, indicated by the following schematic arrangement of their suffixes λ_α:

$$\begin{array}{cccccccc}
\alpha', & \alpha'', & \alpha''', & \cdots, & \alpha^{(i)}, & \cdots, & \alpha^{(n)}, \\
\beta', & \beta'', & \beta''', & . & . & ., & \beta^{(n)}, \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . \\
\omega', & \omega'', & \omega''', & . & . & ., & \omega^{(n)}.
\end{array}$$

Suppose, in addition that the $n\alpha$'s agree in their first h elements $(0 \leqq h < a)$, but not in their $(h+1)$th elements, i. e., $\alpha_i^{(j)} = \alpha'_i$ $(i = 1, 2, \cdots, h$ and $j = 1, 2, \cdots, n)$, but in particular $\alpha''_{h+1} \equiv \alpha'_{h+1} + d$, mod. p, where $d \not\equiv 0$ mod. p.

A substitution P can be found which will transform $L_{\alpha'}$ into $L_{\beta'}$, and at the same time $L_{\alpha''}$ into any L_λ having $l_i = b'_i$ $(i = 1, 2, \cdots, h)$ and

$$l_{h+1} - b'_{h+1} \equiv \alpha''_{h+1} - \alpha'_{h+1} \pmod{p},$$

since

$$\alpha''_{h+1} \not\equiv \alpha'_{h+1}.$$

Hence among the β's every λ must occur having $l_i = b'_i (i = 1, 2, \cdots, h)$, if the division of the letters be into sets of imprimitivity, and accordingly among the α's every λ must occur for which $l_i = a_i (i = 1, 2, \cdots, h)$. This establishes the theorem.

§ 7. *The induced groups on the sets of imprimitivity.*

The substitutions of $\mathfrak{P}^{p^a}$ give us a group of degree p^h of induced substitutions on the p^h sets of imprimitivity of $\mathfrak{P}^{p^a}$ of order h. The *letter* (L'_{μ_λ}) of this group is, or corresponds to, the totality of L_{λ_α} in which $l_i = m_i (i = 1, 2, \cdots, h)$. The h-partite subscripts of the L''s classify them in a scheme corresponding to that of the L's. The substitution upon the L''s induced by E_{λ_g} on the L's is seen 1) if $g \equiv h$ to be the identity, 2) if $g < h$ to be exactly the corresponding generator E'_{λ_g}, of the Sylow subgroup of the symmetric group upon the p^h L''s, defined after the method of § 3, by the classification and ordering set up by the suffixes μ_λ. Hence we have the

THEOREM. The totality of E_{λ_g}'s of $\mathfrak{P}^{p^a}$ $(g = 0, 1, 2, \cdots, h-1)$, generate a subgroup of $\mathfrak{P}^{p^a}$ which is isomorphic to the induced group on the sets of imprimitivity of $\mathfrak{P}^{p^a}$ of order h, and also to a Sylow subgroup of the symmetric group of degree p^h.

From this view-point $\mathfrak{P}^{p^a}$ itself is seen to be but a member of an unending series of intimately related Sylow subgroups of symmetric groups whose degrees are the ascending powers of p.

It is to be observed that E_{λ_g}, applied as a transformer to the totality of E_{λ_h}'s, makes upon them the same substitution as E'_{λ_g} upon the letters, L'_{λ_h}, of its group, $\mathfrak{P}^{p^h}$.

§ 8. *On the cyclic character of the substitutions of* $\mathfrak{P}$.

We proceed to establish relations between the cyclic character of a substitution P of $\mathfrak{P}^{p^a}$ and the various substitutions upon the sets of imprimitivity of $\mathfrak{P}^{p^a}$ induced by P, which we have seen may be thought of as substitutions of Sylow subgroups of symmetric groups whose degrees are the various powers of p less than p^a, or as substitutions upon the E_{λ_h}'s produced by transformation by the substitutions

$$\overline{P}_h = \prod_{g=0,1,\cdots,h-1} \prod_{\lambda_g | \Lambda_g} E_{\lambda_g}^{k_{\lambda_g}}.$$

In addition to the above it will be convenient to adopt the following notations for other portions of the normal expression of P:

$$P_h = \prod_{\lambda_h | \Lambda_h} E_{\lambda_h}^{k_{\lambda_h}},$$

$$\underline{P}_h = \prod_{k=h+1,\cdots,a-1} \prod E_{\lambda_k}^{k_{\lambda_k}}.$$

Thus

$$P = \overline{P}_h \cdot P_h \cdot \underline{P}_h.$$

The substitution upon the E_{λ_h}'s produced by $\overline{P}_h$ will be denoted by $\overline{P}'_h$.

If λ_h is contained in λ_{h+1}, then

$$\overline{P}_h^{-x} E_{\lambda_h} \overline{P}_h^{x} = E'_{\lambda_h},$$

$$\overline{P}_{h+1}^{-x} E_{\lambda_{h+1}} \overline{P}_{h+1}^{x} = E'_{\lambda_{h+1}},$$

where λ'_h is contained in λ'_{h+1} (§ 6). If E_{λ_h}, in the cyclic notation of P'_h, belongs to a cycle with p^h letters, then will

$$\overline{P}_{h+1}^{-p^h} E_{\lambda_{h+1}} \overline{P}_{h+1}^{p^h} = E''_{\lambda_{h+1}},$$

where

1) $$l''_i = l_i \qquad (i = 1, 2, \cdots, h),$$

2) $$l''_{h+1} \equiv l_{h+1} + \sum k_{\mu_h} \pmod{p},$$

the summation being for μ_h running through the suffixes of the E_{μ_h}'s belonging to the cycle of $\overline{P}'_h$ containing E_{λ_h}. If this sum is a multiple of p the cycle of $\overline{P}'_{h+1}$ containing $E_{\lambda_h \lambda_{h+1}}$ contains p^h E's. If it is not a multiple of p, the cycle will contain the p^{h+1} $E_{\mu_h \mu_{h+1}}$'s whose suffixes contain the suffixes of the E_{μ_h}'s in the same cycle as E_{λ_h}. From this follows the

THEOREM. If $\overline{P}'_h$, written in cyclic notation, has a_i cycles each containing p^{b_i} E_{λ_h}'s $(i = 1, 2, \cdots, r)$* and if s_i of the a_i cycles are composed of E_λ's for which the sum of the p^{b_i} k_λ's is congruent to zero, modulo p, then $\overline{P}'_{h+1}$ has, corresponding to these, $p\,s_i$ cycles with p^{b_i} E's in each and $a_i - s_i$ cycles with p^{b_i+1} E's in each.

COROLLARY 1. If n_g denotes the total number of cycles in $\overline{P}'_g$, then in the above

$$n_h = \sum a_i,$$

$$n_{h+1} = n_h + (p-1)\sum_{i=1}^{r} s_i.$$

COROLLARY 2. Since $n_1 = 1$, or p, according as k_0 is not, or is, equal to zero therefore $n_h \equiv 1 \pmod{p-1}$ for all values of h.

If $\overline{P}'_g$ has order p^g and so consists of but one cycle, then every cycle in $\overline{P}'_h$ $(h = g, g+1, \cdots, a)$ will contain at least p^g letters. If P is also of order p^g, then every cycle in each of the $\overline{P}'_h$'s contains precisely p^g letters. Hence upon the choice of the exponents in P_h of such a $P(g \leqq h \leqq a-1)$, there are imposed p^{h-g} conditions giving in all $p^{p^h - p^{h-g}}$ choices of P_g for a given $\overline{P}_h$. From this we derive

COROLLARY 4. The total number of P's of order p^g and having a given $\overline{P}_g$ also of order p^g is p^m, where

$$m = (p^g - 1)\frac{p^{a-g} - 1}{p - 1}.$$

COROLLARY 5. If we denote the order of $\overline{P}'_g$ by p^{π_g}, then $\pi_g \leqq g$; and if $g < h$ we have

$$0 \leqq \pi_h - \pi_g \leqq h - g.$$

Hence if P is of order p^a, the order of $\overline{P}'_g$ is p^g, and we have

COROLLARY 6. The necessary and sufficient condition that P has order p^a is that $\sum k_{\lambda_g} \not\equiv 0$, mod. p, $(g = 0, 1, \cdots, a-1)$, the summation being for λ_g running through Λ_g.

§ 9. *Certain normalizations.*

If $R = P^{-1}$, it can be proved that

$$R_h = (P_h^{-1})_{\bar{n}_h}.$$

* Thus $p^h = \sum_{i=1}^{r} a_i p^{b_i}$.

The symbol

$$A_B$$

is used for $B^{-1}AB$ and it is convenient in such expressions as the above to conceive the operation as performed by a substitution upon the E's, in this case the substitution which we have denoted by R'_λ. It is still better to conceive the effect to be produced by a substitution upon the exponents of the E's in P_λ^{-1}.

In general if $R = P \cdot Q \cdot S \cdots T \cdot U$, then

$$R_\lambda = (P_\lambda)_{Q_\lambda \cdot S_\lambda \cdots T_\lambda} \cdot (Q_\lambda)_{S_\lambda \cdots T_\lambda} \cdots (T_\lambda)_{T_\lambda} \cdot U_\lambda .$$

If $R = Q^{-1}PQ$, then

$$R_\lambda = (P_\lambda)_{Q_\lambda} \cdot (Q_\lambda^{-1})_{R_\lambda} \cdot Q_\lambda .$$

§ 10. *Invariant substitutions.*

Consider $R = E_{\lambda_g}^{-1} P E_{\lambda_g}$. We have

$$\bar{R}_g = P_g ,$$

$$R_g = P_g \cdot (E_{\lambda_g}^{-1})_{P_g} \cdot E_{\lambda_g} .$$

Therefore in order that $R = P$ for every E_{λ_g}, it is necessary and sufficient that every E_{λ_g} should be invariant under P_g. In particular, every $E_{\lambda_{a-1}}$ must be invariant under P_{a-1} and therefore $P_{a-1} = I$ and $P = P_{a-1}$. From the transitivity of $\mathfrak{P}$ it follows that it is necessary (and sufficient) in order that

$$\prod_{\lambda_{a-1} | \Delta_{a-1}} E_{\lambda_{a-1}}^{k_{\lambda_{a-1}}}$$

is invariant under $\mathfrak{P}$, that the exponents k_λ are all equal. Thus we have the

THEOREM. The only invariant substitutions of $\mathfrak{P}^{p^a}$ are the p powers of

$$\prod_{\lambda_{a-1} | \Delta_{a-1}} E_{\lambda_{a-1}} .$$

§ 11. *Substitutions of orders p and p^a.*

It follows from § 8, corollary 6, that the number of elements of $\mathfrak{P}^{p^a}$ of order p^a is

$$\prod_{g=0,\,1,\,\ldots,\,a-1} (p-1)p^{p^g-1} = (p-1)^a p^{a-a} \qquad \left(a = \frac{p^a-1}{p-1}\right).$$

The factor $p-1$ occurs because $p-1$ congruentially distinct values of

$$\sum_{\lambda_g | \Delta_g} k_{\lambda_g}$$

are admissible.

Let P be any substitution of order p^a and Q another, as yet undetermined, substitution of $\mathfrak{P}$. Let $R = Q^{-1} \cdot P \cdot Q$. Then (§ 9)

$$R_h = (P_h)_{\overline{Q}_h} \cdot (Q_h^{-1})_{\overline{R}_h} \cdot Q_h.$$

Let s_h be the least positive residue of the sum of the exponents of the E_{λ_h}'s in P_h, modulo p. We will assume $\overline{Q}_h$ to have been already selected, and therefore

$$(P_h)_{\overline{Q}_h} \qquad \text{and} \qquad \overline{R}_h$$

are determined.

Let

$$(P^h)_{\overline{Q}_h} = \prod_{\lambda_h | \Lambda_h} E_{\lambda_h}^{r_{\lambda_h}}$$

and

$$\overline{R}_h' = (E_{\beta_h'}, E_{\beta_h''}, E_{\beta_h'''}, \cdots, E_{\beta_h^{(p^h)}}).$$

Since $\overline{R}_h'$ is conjugate to $\overline{P}_h'$, it will consist of but one cycle.

If now we denote Q_h, which we wish to determine, by

$$\prod_{\lambda_h | \Lambda_h} E_{\lambda_h}^{y_{\lambda_h}},$$

and

$$(Q_h^{-1})_{\overline{R}_h} Q_h \qquad \text{by} \qquad \prod_{\lambda_h | \Lambda_h} E_{\lambda_h}^{x_{\lambda_h}},$$

then the x's and the y's are related by the congruences

$$x_{\beta_h^{(i)}} \equiv y_{\beta_h^{(i)}} - y_{\beta_h^{(j)}} \pmod{p},$$

in which

$$j \equiv i - 1 \pmod{p^h}$$

and

$$i = 1, 2, 3, \cdots, p^h.$$

There is one, and only one, condition imposed upon the x's, viz., that their sum is congruent to zero, modulo p. This condition is fulfilled by the following choice of the x's:

$$x_{\beta_h^{(i)}} \equiv -v_{\beta_h^{(i)}} \pmod{p} \qquad (i = 2, 3, \cdots, p^h),$$

$$x_{\beta_h'} \equiv s_h - v_{\beta_h'} \pmod{p},$$

since

$$\Sigma v_{\beta_h} \equiv s_h \pmod{p}.$$

We can now solve the above congruences for the y's and so determine a Q_h such that

$$R_h = E_{\beta_h'}^{s_h}.$$

Proceeding thus for $h = 1, 2, \cdots, a-1$ we have finally

$$R = \prod_{h=0, 1, \cdots, a-1} E_{\beta_h'}^{s_h},$$

where β_h is an arbitrarily selected number of Λ_h. No two of these R's for different sets of s_h's are conjugates and hence we have the

THEOREM. There are $(p-1)^a p^{a-\alpha}$ substitutions in $\mathfrak{P}^{p^a}$ of order p^a, where $\alpha = p^{a-1} + p^{a-2} + \cdots + p + 1$. They fall into $(p-1)^a$ sets of conjugates each set containing $p^{a-\alpha}$ substitutions and determined by the set of least positive residues, modulo p, of the various sums

$$\sum_{\lambda_h | \Lambda_h} k_{\lambda_h} \qquad (h = 0, 1, 2, \cdots, a-1).$$

COROLLARY 1. A substitution of order p^a is invariant only under its own powers.

From this theorem and corollary 4 of § 8 we have

COROLLARY 2. There are

$$(p-1)^c p^{p^{a-c} \cdot \frac{p^c-1}{p-1} - c}$$

substitutions, P, in $\mathfrak{P}^{p^a}$ of order p^c and such that $\overline{\mathrm{P}}_c$ is also of order p^c.

In particular for $c = 1$ we have

COROLLARY 3. There are $(p-1)p^{p^{a-1}-1}$ substitutions of order p, for which $k_0 \not\equiv 0 \pmod{p}$.

Every substitution P of $\mathfrak{P}$ having $k_0 = 0$ is the product of p substitutions $\mathrm{P}', \mathrm{P}'', \mathrm{P}''', \cdots, \mathrm{P}^{(p)}$ chosen one from each of the p Sylow subgroups of the symmetric groups on the subsets of the letters of $\mathfrak{P}^{p^a}$, of order 1 (§ 3). If $\mathrm{P}^{p^c} = \mathrm{I}$ then $\mathrm{P}^{(i)p^c} = \mathrm{I}$ $(i = 1, 2, \cdots, p)$, and conversely. Therefore the total number of substitutions in $\mathfrak{P}^{p^a}$ whose orders are less than or equal to p^c and having $k_0 = 0$ is equal to the pth power of the number of substitutions in $\mathfrak{P}^{p^{a-1}}$ of orders less than or equal to p^c.

Hence, for $c = 1$, we have from corollary 3,

THEOREM. The total number of substitutions in $\mathfrak{P}^{p^a}$ of order p is the value of n_a determined by the following recursion formula:

$$n_h = (p-1)p^{p^{h-1}-1} + (n_{h-1}+1)^p - 1,$$
$$n_1 = p - 1.$$

§ 12. *The set of Sylow subgroups of* $\mathfrak{S}^{p^a}$.

Any substitution G of $\mathfrak{S}$ which transforms $\mathfrak{P}$ into itself must conform to the complete system of imprimitivity of $\mathfrak{P}$. For let

$$\begin{array}{cccccc} \alpha', & \alpha'', & \alpha''', & \cdots, & \alpha^{(p^h)} \\ \beta', & \beta'', & \beta''', & \cdots, & \beta^{(p^h)} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}$$

indicate a division of the letters L_{λ_α} into imprimitive sets (cf. § 6). The row $\alpha', \alpha'', \cdots$ consists of the totality of λ_α's agreeing with α' in their first p^{n-h} elements and similarly for each of the other rows. Suppose that G transforms this tactical arrangement of the letters into another having two letters from different rows above in the same row, e. g.,

$$\begin{array}{llll} \alpha', & \beta', & \alpha''', & \cdots \\ \alpha'', & \gamma', & \ldots & \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{array}$$

Now $G^{-1}PG$ will transform this second arrangement in the same way that P transforms the first. Since α' and β' agree in their first g elements, where $g < a - h$, it is possible to find a P' which will transform $L_{\alpha'}$ into $L_{\alpha''}$ and $L_{\beta'}$ into any one of n letters where $n \geqq p^h$ and therefore $L_{\beta'}$ into a letter whose suffix does not occur in the same row of the second arrangement as α''. Taking $P = GP'G^{-1}$ we see that the hypothesis leads to a contradiction.

Hence the substitution G upon the letters L_{λ_α} may be thought of as produced by changing, first the initial elements of their suffixes, then the second elements, then the third and so on, the change produced in any one class of elements being a function of the preceding ones only. Let

$$\text{(I)} \qquad \begin{pmatrix} 1, & 2, & 3, & \cdots, & p \\ b_1, & b_2, & b_3, & \cdots, & b_p \end{pmatrix}$$

be the substitution upon the first elements of the suffixes induced by G. Then since $G^{-1}E_0G$ produces upon the L's, as rearranged by G, the same substitution as E_0 produced upon the preceding arrangement,

$$\text{(II)} \qquad b_2 - b_1 \equiv b_3 - b_2 \equiv \cdots \equiv b_1 - b_p \equiv k_0 \,(\text{mod. } p),$$

where k_0 is the exponent of E_0 in the normal form of $G^{-1}E_0G$ (§ 4). The group $\mathfrak{P}$ is invariant under G_0, the substitution upon the L's induced by (I) where the b's are any solution of the congruences (II) k_0 being any one of the integers $1, 2, \cdots, p-1$. There are $p(p-1)$ solutions.

The substitution $G' = G_0^{-1}G$ will also leave $\mathfrak{P}$ invariant and is the product of p substitutions of degree $p^{\alpha-1}$ each of which may be discussed in relation to a $\mathfrak{P}^{p^{\alpha-1}}$ as G has been in relation to $\mathfrak{P}^{p^\alpha}$. In this way G is found to be the product of $1 + p + p + \cdots + p^{\alpha-1}$ substitutions under each of which $\mathfrak{P}$ is invariant and for each of which there are $p(p-1)$ choices. Hence the total number of substitutions of $\mathfrak{S}^{p^\alpha}$ under which $\mathfrak{P}^{p^\alpha}$ is invariant is

$$\{p(p-1)\}^\alpha \qquad \left(\alpha = \frac{p^\alpha - 1}{p-1}\right).$$

If in all the congruences (II) we take $k_0 = 1$ the G thus obtained is a substitution of $\mathfrak{P}$ and we so obtain all the substitutions of $\mathfrak{P}$. If $k_0 \neq 1$ the corresponding E, (E_0), is not invariant under G. If in § 9 we take $P = E_{\lambda_g}$ and Q any substitution of $\mathfrak{P}$, it is seen that the necessary and sufficient condition that the system of generators of $\mathfrak{P}$ should be invariant under Q is that Q_h should be invariant under every

$$E_{\lambda_g} \quad (g = 0, 1, \cdots, h-1; h = 1, 2, \cdots, a-1).$$

This requires that the exponents of the E's in Q_h shall be all equal. The subgroup of $\mathfrak{G}$, or of $\mathfrak{S}$, consisting of substitutions leaving the set of generators of $\mathfrak{P}$ invariant is of order p^a and consists of the subgroup of $\mathfrak{P}$ generated by the substitutions

$$\prod_{\lambda_g | \Delta_g} E_{\lambda_g} \qquad (g = 0, 1, \cdots, a-1).$$

The subgroup of $\mathfrak{S}$ and overgroup of $\mathfrak{G}$ consisting of all the substitutions leaving invariant the complex classification of the letters given by the imprimitivity of $\mathfrak{P}$ is readily seen to be of order $(p!)^a$.

THEOREM. There are $p^a!/p^a(p-1)^a$ Sylow subgroups of the symmetric group, they fall into $p^a!/(p!)^a$ classes each containing $\{(p-2)!\}^a$ groups having the same system of imprimitivity. Each group has $p^{a-1} \cdot (p-1)^a$ systems of generators of the type used in this paper, where

$$\alpha = p^{a-1} + p^{a-2} + \cdots + p + 1.$$

§ 13. *Sylow subgroups of lower degree contained in* $\mathfrak{P}$.

In obtaining $\mathfrak{P}^{p^a}$ we required and obtained (§ 3), as subgroups of it p^{a-h} Sylow subgroups of the symmetric groups of degree p^h on the various subsets of the letters of order h $(h = 1, 2, \cdots, a-1)$. They consist of the totality of substitutions of $\mathfrak{P}^a$ affecting only the letters of the corresponding subset of order h and are readily seen to be all conjugate and to form a complete system.

These are the only subgroups of $\mathfrak{P}^{p^a}$ which are Sylow subgroups of symmetric groups of degree p^h. For if such a subgroup, $\mathfrak{G}_1$, affected two letters L and L′ from different subsets of order h, because of its transitivity $\mathfrak{G}$ must contain a substitution G which transform L into L′. Then, on account of the imprimitivity of $\mathfrak{P}$, G must affect at least $2p^h$ letters. Therefore the degree of $\mathfrak{G}$ must be greater than or equal to $2p^h$ contrary to the assumption.

§ 14. *The maximal invariant abelian subgroup of* $\mathfrak{P}$ *and a series of invariant subgroups.*

In order that a group $\mathfrak{B}$ should be an invariant abelian subgroup of $\mathfrak{P}$ it is necessary that the division of the letters into subsets of order $a-1$ (§ 3) should

constitute a system of intransitivity of $\mathfrak{B}$. For if some B transforms L_{α_a} into L_{β_a} of a different subset of order $a-1$, i. e., α_a and β_a do not agree in their first $a-1$ elements, then

$$A = E_{\alpha_{a-1}}^{-1} B^{-1} E_{\alpha_{a-1}} \cdot B \cdot E_{\alpha_{a-1}}^{-1} B E_{\alpha_{a-1}} = B \cdot E_{\beta_{a-1}}^{-1} \cdot E_{\gamma_{a-1}} \cdot E_{\beta_{a-1}}^{-1} \cdot E_{\alpha_{a-1}} \neq B$$

and therefore $\mathfrak{B}$ is not an invariant abelian subgroup of $\mathfrak{P}$.

The group generated by the substitutions $E_{\lambda_{a-1}}$ $(\lambda_{a-1}|\Lambda_{a-1})$, and consisting of the totality of substitutions of $\mathfrak{P}$ having the particular system of imprimitivity of $\mathfrak{P}$, which has p letters in each division, as their system of intransitivity, is readily seen to be both invariant and abelian and therefore, by the above, the maximal invariant abelian subgroup of $\mathfrak{P}$. We will denote it by $\mathfrak{D}_{(a-1)}$. Its order is $p^{p^{a-1}}$. The substitutions of $\mathfrak{P}$ generated by the remaining E's constitute a system of left extenders of $\mathfrak{D}_{(a-1)}$ to $\mathfrak{P}$ (cf. § 4) and therefore the quotient group $\mathfrak{P}/\mathfrak{D}_{a-1}$ is simply isomorphic to a Sylow subgroup on p^{a-1} letters (L') obtained from $\mathfrak{P}$ by establishing a correspondence between the L''s and the subsets of order $a-1$ of the letters of $\mathfrak{P}$ (cf. § 7).

THEOREM. The series of subgroups $\mathfrak{D}_0 = \mathfrak{P}, \mathfrak{D}_{(1)}, \mathfrak{D}_{(2)}, \cdots, \mathfrak{D}_{(a-1)}, \mathfrak{D}_{(a)} = I$, in which $\mathfrak{D}_{(h)}$ consists of the totality of substitutions having the system of imprimitivity of $\mathfrak{P}$ containing p^{a-h} letters in each division as a system of intransitivity, or which, in their normal form (§ 4), have $k_{\lambda_g} = 0$ $(g = 0, 1, \cdots, h-1)$, are each contained in, and invariant under, every preceding one. The quotient group $\mathfrak{P}/\mathfrak{D}_{(h)}$ is simply isomorphic to a Sylow subgroup on p^h letters, the one derived in § 7, and $\mathfrak{D}_{(h-1)}/\mathfrak{D}_{(h)}$ is the maximal invariant abelian subgroup of $\mathfrak{P}/\mathfrak{D}_{(h)}$. In particular $\mathfrak{D}_{(a-1)}$ is the maximal invariant abelian subgroup of $\mathfrak{P}$.

§ 15. *The commutator series of subgroups.*

It has been proved* that, if $P_1, P_2, \cdots, P_k$ be a set of generators of group $\mathfrak{P}$ and $G_{ij} = P_i^{-1} P_j^{-1} P_i P_j$, as i and j have, independently, the range $1, 2, 3, \cdots, k$, generate a subgroup $\mathfrak{G}$, then the smallest invariant subgroup of $\mathfrak{P}$ containing $\mathfrak{G}$ is the first commutator subgroup of $\mathfrak{P}$. Applying this to the Sylow subgroup with the generators E_{λ_h} for the G's we have, besides the identity, products of the form

$$E_{\lambda_h'}^{-} E_{\lambda_h},$$

where $l_i' = l_i$ for all values of i from 1 to h excepting one, say d, and $l_d' \equiv l_d \pm 1$, mod. p. Also any product of this form can be obtained in this way.

By combinations of these products we can generate any substitution of $\mathfrak{P}$ whose normal form (§ 4) satisfies the a conditions

$$\sum_{\lambda_g | \Lambda_g} k_{\lambda_g} \equiv 0 \pmod{p} \qquad (g = 0, 1, 2, \cdots, a-1).$$

It is easily seen (cf. § 9) that any product of substitutions satisfying these con-

* MILLER, Bulletin, American Mathematical Society, vol. 4 (1898), p. 136.

ditions, and also the transform of such a substitution by any substitution of $\mathfrak{P}$, satisfy the same congruence. Hence the

THEOREM. The totality of substitutions whose normal forms satisfy the above congruences constitutes the first commutator subgroup of $\mathfrak{P}$, which we shall denote by $\mathfrak{C}_1$. The order of $\mathfrak{C}_1$ is $p^{a-\alpha}$ $(\alpha = p^{a-1} + p^{a-2} + \cdots + p + 1)$.

The first commutator subgroup of $\mathfrak{P}$ is intransitive with the sets of imprimitivity of $\mathfrak{P}$ containing p^{a-1} letters in each as its sets of intransitivity. It is independently simply transitive within any $p-1$ of its sets of intransitivity.

Since in the normal form of $\mathfrak{C}_1$ we have $k_0 = 0$, it follows (cf. § 9) that when we normalize any product of commutators of $\mathfrak{C}_1$ the exponents in the result fulfil the $1 + p(a-1)$ conditions

$$k_0 = 0, \qquad \sum k_{\lambda_g} \equiv 0 \pmod{p} \quad (g = 1, 2, 3, \cdots, a-1),$$

the summation being for all the numbers of Λ_g with a chosen value for l_1. The group $\mathfrak{C}_2$, consisting of the totality of such substitutions of $\mathfrak{P}$, is the product of the first commutator subgroups of the various Sylow subgroups of degree p^{a-1} contained in $\mathfrak{P}$.

Among the substitutions of $\mathfrak{C}_1$ occur all the substitutions of the form

$$\mathrm{F} = \mathrm{E}_{\lambda_h}^{-1} \cdot \mathrm{E}_{\lambda_h'},$$

where λ_h and λ_h' are any two numbers of Λ_h such that $l_1 \neq l_1'$ and $1 < h \leqq a-1$. From the above it follows that $\mathfrak{C}_1$ contains a substitution C such that:

$$\mathrm{C}^{-1}\mathrm{E}_{\lambda_h}\mathrm{C} = \mathrm{E}_{\lambda_h},$$

$$\mathrm{C}^{-1}\mathrm{E}_{\lambda_h'}\mathrm{C} = \mathrm{E}_{\lambda_h''},$$

where λ_h'' is any number of Λ_h subject to the one condition that $l_1'' = l_1'$.

Then

$$\mathrm{C}^{-1}\mathrm{F}^{-1}\mathrm{C}\mathrm{F} = \mathrm{E}_{\lambda_h}\mathrm{E}_{\lambda_h''}^{-1}\mathrm{E}_{\lambda_h}^{-1}\mathrm{E}_{\lambda_h'} = \mathrm{E}_{\lambda_h''}'\mathrm{E}_{\lambda_h'}'.$$

These last products, which are commutators of $\mathfrak{C}_1$, generate $\mathfrak{C}_2$, which is therefore the first commutator subgroup of $\mathfrak{C}_1$ or the second commutator subgroup of $\mathfrak{P}$.

By successive application of these results we obtain the

THEOREM. The dth commutator subgroup $(\mathfrak{C}_d)$ of $\mathfrak{P}$ is the product of the first commutator subgroups of the Sylow subgroups of degree p^{a-d+1} contained in $\mathfrak{P}$. It is also the product of the $(d-1)$th commutator subgroups of the p Sylow subgroups of degree p^{a-1} contained in $\mathfrak{P}$. The order of $\mathfrak{C}_d$ is p^{δ}, where

$$\delta = p^{a-1} + p^{a-2} + \cdots p^d - (a-d)p^{d-1}.$$

The cogredient subgroup of $\mathfrak{P}$ (§ 10) is a subgroup of each of the commutator subgroups $\mathfrak{C}_1, \mathfrak{C}_2, \cdots, \mathfrak{C}_{a-1}$.

COLUMBIA UNIVERSITY, NEW YORK.

ON THE SMALLER PERTURBATIONS OF THE LUNAR ARGUMENTS*

BY

ERNEST WILLIAM BROWN

The problem of finding the effects of planetary action on the motion of the moon has not yet been satisfactorily solved. As far as periodic terms are concerned the works of HILL,† NEWCOMB‡ and RADAU§ have tended to considerably shorten and simplify the calculation, reducing it, when once the disturbing function has been computed, to some simple substitutions in a general formula. But the method is not available for finding the non-periodic changes produced on the mean motions of the perigee and node. I propose to obtain here some simple formulæ which permit these perturbations to be found quickly and with all the accuracy that can be desired. The results will be applied to the effects produced by planetary action and by the figure of the earth, but certain of the constants whose values are given below are available for the calculations of any non-periodic perturbations of the perigee and node. The notation adopted here is, in general, that of my paper "On the formation of the derivatives of the lunar coördinates with respect to the elements"‖; the investigation below is, in fact, a continuation of that paper to a certain extent.

(i) *Formulae for finding the non-periodic perturbations of the perigee and node.*

1. The motion of the moon under the attractions of the earth and the sun considered as particles is supposed to have been found. The coördinates are thus expressed in trigonometric series of the angles w_4, w_5, w_6 and an angle not

* Presented to the Society February 27, 1904. Received for publication February 26, 1904.

† *On certain lunar inequalities due to the action of Jupiter*, Washington Astronomical Papers, vol. 3 (1891), pp. 373–393.

‡ *Action of the Planets on the Moon*, Washington Astronomical Papers, vol. 5 (1894), pp. 101–295.

§ *Recherches concernant les inégalités planétaires du mouvement de la lune*, Annales de l'Observatoire de Paris (Mémoires), vol. 21 (1892), pp. 1–114.

‖ Transactions of the American Mathematical Society, vol. 4 (1903), pp. 234–248. This paper will be referred to below by the letter F.

containing the constants of integration, with coefficients depending on constants of integration c_1, c_2, c_3 and known constants. The angles w_j are of the form

$$w_4 = b_4 t + \epsilon, \qquad w_5 = b_5 t + \pi, \qquad w_6 = b_6 t + \theta,$$

where $b_4 = n$, is the mean motion and b_5, b_6 are the mean motions of the perigee and node; the b_i are functions of the c_i and known constants; ϵ, π, θ are the other three constants of integration. The c_i, w_j are called below the "elements" of the moon's motion.

If a new small disturbing function λR be added, the resulting changes in lunar elements are obtained by solving the equations (F., art. 18)

$$(1) \qquad \frac{dc_i}{dt} = \lambda \frac{\partial R}{\partial w_{i+3}}, \qquad \frac{dw_j}{dt} = -\lambda \frac{\partial R}{\partial c_{j-3}} + b_j \qquad (i=1,2,3;\ j=4,5,6).$$

In all practical cases squares of λ may be neglected so that the undisturbed values of the elements may be substituted in the derivatives of R, — a fact which enables us to substitute for R its constant term when R is expanded in a trigonometric series, for we are only concerned here with the constant parts of dw_j/dt. We therefore use the letter R henceforward to denote the constant term of that function.

The equations (1) can now be solved and they give

$$c_i = \text{const.}, \qquad w_j = -\lambda t \frac{\partial R}{\partial c_{i-3}} + b_j t + \text{const.}$$

The theory is at first supposed to be expressed, not in terms of w_j, c_i, but in terms of w_j and n, c_2, c_3, the semi-canonical system (F., art. 10): c_2 contains the square of the eccentricity constant as a factor, and c_3 that of the inclination constant. Let δn, δc_2, δc_3 be the changes in n, c_2, c_3 caused by λR and δb_j the changes in the b_j. Then, since $b_4 = n$,

$$\delta b_4 = -\lambda \frac{\partial R}{\partial c_1} + \delta n,$$

$$\delta b_5 = -\lambda \frac{\partial R}{\partial c_2} + \frac{\partial b_5}{\partial n}\delta n + \frac{\partial b_5}{\partial c_2}\delta c_2 + \frac{\partial b_5}{\partial c_3}\delta c_3,$$

$$\delta b_6 = -\lambda \frac{\partial R}{\partial c_3} + \frac{\partial b_6}{\partial n}\delta n + \frac{\partial b_6}{\partial c_2}\delta c_2 + \frac{\partial b_6}{\partial c_3}\delta c_3.$$

The old definition of the letter n is to be retained, that is, it is to represent the mean motion; thus $\delta b_4 = 0$ and $\delta n = \lambda \partial R/\partial c_1$. We shall, for the present, define c_2, c_3 to be the same as when $\lambda = 0$, so that $\delta c_2 = 0$, $\delta c_3 = 0$. These

definitions are possible because c_1, c_2, c_3 are constant whether λ is zero or not. Hence

$$\delta b_5 = -\lambda\left(\frac{\partial R}{\partial c_2} - \frac{\partial b_5}{\partial n}\frac{\partial R}{\partial c_1}\right), \qquad \delta b_6 = -\lambda\left(\frac{\partial R}{\partial c_3} - \frac{\partial b^2}{\partial n}\frac{\partial R}{\partial c_6}\right),$$

where b_5, b_6 are expressed in terms of n, c_2, c_3 and R is expressed in terms of c_1, c_2, c_3.

I have shown (F., no. 10) that

$$-\frac{\partial b_5}{\partial n} = \frac{\partial c_1}{\partial c_2}, \qquad -\frac{\partial b_6}{\partial n} = \frac{\partial c_1}{\partial c_3},$$

where b_2, c_1 are expressed in terms of n, c_2, c_3. Hence

$$\delta b_5 = -\lambda\frac{\partial R}{\partial c_2}, \qquad \delta b_6 = -\lambda\frac{\partial R}{\partial c_3}, \tag{2}$$

where R is now expressed in terms of n c_2, c_3.

These are the required expressions for δb_5, δb_6.

3. The results (2) are remarkable in that they show the greater simplicity obtained by using the semi-canonical system n, c_2, c_3 instead of the canonical system c_1, c_2, c_3; a similar result was found in another connection (F., art. 10). Moreover, the main difficulty in obtaining accuracy, namely, the formation of derivatives with respect to n, has disappeared. One or two transformations are all that are necessary in order to calculate δb_5, δb_6 with good accuracy from a numerical theory and with complete accuracy from a theory in which the numerical value of the ratio of the mean motions is substituted while the other constants are left in a literal form. The results of my theory are therefore immediately available when the derivatives of R with respect to c_2, c_3 have been expressed in terms of derivatives with respect to e, k—the constants of the theory.

In the applications it is never necessary to go beyond the second powers of the eccentricities and inclinations, and all the functions considered are expansible in *squares* of these quantities and of the ratio of the parallaxes; the square of this latter ratio is negligible. As we have to form derivatives with respect to c_2, c_3, that is, with respect to e^2, k^2, it will be necessary, for this degree of accuracy, to find the expansions as far as the second powers and products of e^2, e'^2, k^2.

4. We have, when the independent variables b_1, c_2, c_3 are changed to b_1, e^2, k^2,

$$\frac{\partial R}{\partial \mathrm{e}^2} = \frac{\partial R}{\partial c_2}\frac{\partial c_2}{\partial \mathrm{e}^2} + \frac{\partial R}{\partial c_3}\frac{\partial c_3}{\partial \mathrm{e}^2}, \qquad \frac{\partial R}{\partial \mathrm{k}^2} = \frac{\partial R}{\partial c_2}\frac{\partial c_2}{\partial \mathrm{k}^2} + \frac{\partial R}{\partial c_3}\frac{\partial c_3}{\partial \mathrm{k}^2},$$

where $\partial/\partial \mathrm{e}^2$, $\partial/\partial \mathrm{k}^2$ denote derivatives with respect to e^2, k^2. Since c_2 contains

the factor e^2, and c_3 the factor k^2, we obtain from (2), on omitting the terms of an order higher than the second,

$$-\frac{\delta b_5}{\lambda} = \frac{\partial R}{\partial c_2} = \frac{\dfrac{\partial R}{\partial e^2}}{\dfrac{\partial c_2}{\partial e^2}} - \frac{\dfrac{\partial R}{\partial k^2}\dfrac{\partial c_3}{\partial e^2}}{\dfrac{\partial c_2}{\partial e^2}\dfrac{\partial c_3}{\partial k^2}},$$

with a similar equation for δb_6.

When R, c_2, c_3 are expanded in powers of e^2, e'^2, k^2, in the form

$$R = n^2a^2\left[R(0) + e^2R(e^2) + k^2R(k^2) + \cdots\right],$$
$$c_2 = na^2\left[e^2c_2(e^2) + e^4c_2(e^4) + e^2e'^2c_2(e^2e'^2) + \cdots\right],$$
$$c_3 = na^2\left[k^2c_3(k^2) + k^4c_3(k^4) + e^2k^2c_3(e^2k^2) + \cdots\right],$$

where $R(0), \cdots, c_2(e^2), \cdots, c_3(k^2), \cdots$ are functions of n'/n only and therefore numerical coefficients, we obtain finally

$$-\frac{\delta b_5}{\lambda u} = \frac{R(e^2)}{c_2(e^2)}\left[1 - \frac{2e^2c_2(e^4) + k^2c_2(e^2k^2) + e'^2c_2(e^2e'^2)}{c_2(e^2)}\right] - k^2\frac{R(k^2)c_3(e^2k^2)}{c_2(e^2)c_3(k^2)} + \frac{2e^2R(e^4) + k^2R(e^2k^2) + e'^2R(e^2e'^2)}{c_2(e^2)}, \tag{3}$$

with a similar expression for δb_6 in which c_3, c_2, k, e are respectively put for c_2, c_3, e, k.

These expressions are not completely accurate to the orders given owing to the final definitions of e, k. These constants are defined by means of the principal elliptic inequality and the principal term in latitude respectively. In general the periodic terms in R will produce in the coefficients of these terms additional parts of the form $\lambda\alpha_0 e$, $\lambda\beta_0 k$ where α_0, β_0 are numerical coefficients. In order to reduce to the final definitions it is therefore necessary to replace e by $(1 - \lambda\alpha_0)e$, k by $(1 - \lambda\beta_0)k$. The change in δb_2 is therefore

$$-2\frac{\partial b_5}{\partial e^2}\lambda\alpha_0 e^2 - 2\frac{\partial b_5}{\partial k^2}\lambda\beta_0 k^2.$$

As $\partial b_5/\partial e^2$, $\partial b_5/\partial k^2$ are of the order $(n'/n)^2$ at least, the orders of these additional parts relatively to the corresponding parts of order e^2, k^2 already found, are in the ratio $(n'/n)^2 : 1$. A similar remark holds in the case of δb_6. In no actual case do these portions give additions to the annual mean motions so great as 0″.005; they therefore can and will be neglected. These additional parts, however, do not violate the general theorem of this paper, namely, that algebraical developments in powers of n'/n are not required, for the coefficients α_0, β_0 can be obtained without such developments (F).

5. The following numerical values are needed:

$$\frac{c_2}{na^2} = -.11845\,\mathrm{e}^2 - .02324\,\mathrm{e}^4 - .26363\,\mathrm{e}^2\mathrm{k}^2 - .00110\,\mathrm{e}^2 e'^2,$$

$$\frac{c_3}{na^2} = -2.00206\,\mathrm{k}^2 - 1.96376\,\mathrm{k}^4 - .28546\,\mathrm{e}^2\mathrm{k}^2 - .00568\,e'^2\mathrm{k}^2;$$

$$n = 17325594'';$$

$$\mathrm{e} = .10983, \qquad \mathrm{k} = .044892, \qquad e' = .01677.$$

The values of c_2, c_3 have been found by the method given in F., art. 11.

The relations between my constants and those (e, γ) of DELAUNAY's theory, though not needed here, may be given:

$$\mathrm{e} = +2.00054\,e - .36682\,e^3 - 2.01160\,e\gamma^2 + .04873\,ee'^2,$$

$$\mathrm{k} = +1.00013\,\gamma - .49609\,\gamma^3 - .49924\,\gamma e^2 - .00037\,\gamma e'^2.$$

(ii) *Application to planetary action.*

6. Let x, y, z be the coördinates of the moon, ξ, η, ζ those of a planet referred to moving axes of x, y in the plane of the ecliptic of which the x-axis points to the mean place of the sun, and an axis perpendicular to this plane. Then if $r^2 = x^2 + y^2 + z^2$, $D^2 = \xi^2 + \eta^2 + \zeta^2$ and λ denotes the mass of the planet, we have, neglecting the ratio of the parallax of the sun to that of the moon,

$$R = \tfrac{3}{2}\frac{(x\xi + y\eta + z\zeta)^2}{D^5} - \tfrac{1}{2}\frac{r^2}{D^3}.$$

It will tend to simplicity if we neglect at the outset certain quantities whose squares are certainly negligible in the results; these are the solar eccentricity and the product of the inclinations of the planet and the moon to the ecliptic. As the constant term in R is alone required we can further neglect the products $xy\xi\eta/D^5$, $xz\xi\zeta/D^5$, $yz\eta\zeta/D^5$. The function then can be put into the form:

$$R = \tfrac{1}{4}(x^2 + y^2 - 2z^2)\left(\frac{1}{D^3} - \frac{3\zeta^2}{D^5}\right) + \tfrac{3}{4}(x^2 - y^2)\frac{\xi^2 - \eta^2}{D^5}$$

$$= \tfrac{1}{4}(us - 2z^2)_0\left(\frac{1}{D^3} - \frac{3\zeta^2}{D^5}\right)_0 + \tfrac{3}{8}(u^2 + s^2)_0\left(\frac{\xi^2 - \eta^2}{D^5}\right)_0$$

where $u = x + y\sqrt{-1}$, $s = x - y\sqrt{-1}$, and $(\ )_0$ denotes the constant term in the expansion of the included function. The separation of the parts depending on the coördinates of the moon from those depending on the coördinates of the planet is possible because when the solar eccentricity is neglected, they have no common angles.

Let n', a', be the mean motion and mean distance of the sun; n, a, those of the moon; m', the mass of the sun; $m = n'/(n - n')$; a, a certain constant which differs little from a;

$$H = \frac{\lambda}{m'}\left(\frac{a'^3}{D^3} - \frac{3\zeta^2 a'^3}{D^5}\right)_0, \qquad K = \frac{\lambda}{m'}a'^3\left(\frac{\xi^2 - \eta^2}{D^5}\right)_0;$$

then, since $(u^2)_0 = (s^2)_0$, the expression for R may be written

$$\lambda R = \frac{\mathrm{m}^2}{(1+\mathrm{m})^2}\frac{\mathrm{a}^2}{a^2}n^2a^2\left[\tfrac{1}{4}H\left(\frac{us - 2z^2}{\mathrm{a}^2}\right)_0 + \tfrac{3}{4}K\left(\frac{u^2}{\mathrm{a}^2}\right)_0\right].$$

In this expression the only parts containing e, k are the coefficients of H, K within the square brackets. I already have the results for these since they were required in obtaining the motion in the main problem. I find

$$\left(\frac{us - 2z^2}{\mathrm{a}^2}\right)_0 = \cdots + .38229\,\mathrm{e}^2 - 6.00851\,\mathrm{k}^2 + .0398\,\mathrm{e}^4 - 3.0395\,\mathrm{e}^2\mathrm{k}^2 + .0053\,\mathrm{k}^4 + \cdots,$$

$$\left(\frac{u^2}{\mathrm{a}^2}\right)_0 = \cdots + .25496\,\mathrm{e}^2 + .18030\,\mathrm{k}^2 - .0142\,\mathrm{e}^4 - .4094\,\mathrm{e}^2\mathrm{k}^2 - .2035\,\mathrm{k}^4 + \cdots.$$

7. We must next calculate H, K. First, owing to the numerical values of the eccentricities, inclinations and masses of the planets, the only possible sensible effect of the eccentricities and inclinations is the inclination of Venus. Let then V'', V' be the mean longitudes of a planet and the sun, a'', a' their mean distances, γ'' the sine of half inclination of the planet's orbit to the elliptic, h'' the longitude of the planet's node. Then, omitting powers of γ'' beyond the second,

$$\xi = -a' + (1 - \gamma''^2)a''\cos(V'' - V') + \gamma''^2 a''\cos(V'' + V' - 2h''),$$

$$\eta = (1 - \gamma''^2)a''\sin(V'' - V') - \gamma''^2 a''\sin V'' + V' - 2h''),$$

$$\zeta = 2\gamma'' a''\sin(V'' - h'');$$

$$D^2 = a'^2 + a''^2 - 2a'a''(1 - \gamma''^2)\cos(V'' - V') - 2\gamma''^2 a'a''\cos(V'' + V' - 2h'')$$

$$= D_0^2 - 2\gamma''^2 a'a''(V'' + V' - 2h''),$$

$$\xi^2 - \eta^2 = a'^2 - 2a'a''(1 - \gamma''^2)\cos(V'' - V') + a''^2(1 - 2\gamma''^2)\cos 2(V'' - V') - 2\gamma''^2 a''\{a'\cos(V'' + V' - 2h'') - a''\cos 2(V' - h'')\},$$

$$\zeta^2 = 2\gamma''^2 a''^2\{1 - \cos 2(V'' - h'')\}.$$

Let

$$D^{-n}a'^{n} = A_0^{(n)} + 2A_1^{(n)}\cos(V''-V') + 2A_2^{(n)}\cos 2(V''-V') + \cdots.$$

Then

$$H = \frac{\lambda}{m'}\left(A_0^{(3)} - 6\gamma''^2\frac{a''^2}{a'^2}A_0^{(5)}\right),$$

$$K = \frac{\lambda}{m'}\left(A_0^{(5)} - 2(1-\gamma''^2)\frac{a''}{a'}A_1^{(5)} + (1-2\gamma''^2)\frac{a''^2}{a'^2}A_2^{(5)}\right).$$

The following table gives the values of the various quantities:

Planet.	Mercury.	Venus.	Mars.	Jupiter.	Saturn.
$\frac{m'}{\lambda}$	6000000	408000	3093500	1047.35	3501.6
$\log\frac{a''}{a'}$	9.5878	9.85934	.1829	.71623	.9795
$A_0^{(3)}$	1.4359	4.9317	1.0858	$10^{-3}\times 7.7267$	$10^{-3}\times 1.181$
$A_0^{(5)}$	2.5658	41.9340	2.3140	$10^{-4}\times 3.3035$	$10^{-5}\times 1.356$
$A_1^{(5)}$	1.9560	40.7575	2.2042	$10^{-4}\times 1.4856$	$10^{-6}\times 3.483$
$A_2^{(5)}$	1.2086	37.8764	1.9597	$10^{-5}\times 4.8834$	$10^{-7}\times 6.35$

Of these numbers, the values of the masses are taken from the best modern determinations; the ratios of the mean distances are certain to the degree of accuracy required here; the values of $A_i^{(n)}$ for Venus and of $A_0^{(3)}$ for Mars have been calculated from the tables given by Newcomb;* the rest of the numbers are taken from the corresponding table of Hansen.†

It is directly seen that the inclination of Venus exerts a slight effect. For since $\gamma'' = .0296$, the ratio of the second term of H to the first is $1/43$, and the part produced by the first term is about $1''$ as we shall see in the following table. The effect on K is smaller.

* *Action of the Planets on the Moon*, Washington Astronomical Papers, vol. 5 (1894), pp. 248–261.

† *Darlegung der theoretischen Berechnung der in den Mondtafeln angewandten Störungen* (Abh. 1), Abhandlungen der mathematisch-physischen Classe der Königlich Sächsischen Gesellschafte der Wissenschaften, vol. 6 (1862), p. 487. The table above is not quite consistent for the values $A_i^{(n)}$ for Venus and that of $A_0^{(3)}$ for Mars include the squares of the inclinations and eccentricities of those planets, while the other $A_i^{(n)}$ do not. But as all these squares are negligible, except that of the inclination of Venus, the slight inconsistency makes no difference in the results.

8. The results of the calculations are as follows:

Planet.	$10^8 H$	Part from H.		$10^8 K$	Part from K.	
		δb_5	δb_6		δb_5	δb_6
Mercury,	+ 24	+ 0″.018	− 0″.017	+ 20.6	+ 0″.031	+ 0″.001
Venus,	1181	.906	.860	687.9	1.060	.041
Mars,	35	.027	.025	4.7	.007	.000
Jupiter,	738	.566	.537	10.2	.016	.001
Saturn,	34	.026	.025	0.0	.000	.000
Sums,	+ 2012	+ 1″.543	− 1″.464	+ 723.4	+ 1″.114	+ 0″.043

The complete annual mean motions contributed by direct planetary action are therefore

$$\delta b_5 = + 2''.66, \qquad \delta b_6 = - 1''.42.$$

In order to show the degree of accuracy obtained by the method, I give the parts of these contributed by e^2, k^2. They are:

in δb_5, from H, by e^2, − 0″.004; by k^2, − 0″.025;
" " " K, " − 0″.005; " − 0″.009;
" δb_6, " H, " − 0″.009; " + 0″.006;
" " " K, " − 0″.003; " .000.

The parts independent of e^2, k^2 have also been calculated directly by the method of my lunar theory, and the results agree exactly, as they should, with those obtained above.

(iii) *Application to the action arising from the figure of the earth.*

9. The disturbing function has been fully expanded by HILL.* The only terms which will produce constant portions are, in his notation,

$$\frac{\beta_1}{a^3}\mu\left[\tfrac{1}{3} - 2\gamma^2 + 2\gamma'\right]\frac{a^3}{r^3} + 2\frac{\beta_1\mu}{a^3}\left[\gamma^2 - \gamma'\right]\frac{a^3}{r^3}\cos 2v,$$

or, in rectangular coördinates,

$$\lambda R_0 = \lambda n^2 a^2\left[\frac{a^3}{3r^3} - \frac{z^2 a^3}{r^5}\right]_0, \qquad \lambda = \frac{\beta_1}{a^2},$$

where $r^2 = x^2 + y^2 + z^2$. In this expression λ is a small coefficient determined from observation. I shall here adopt HILL's value† for it, since for any other

*G. W. HILL, *Determination of the inequalities in the moon's motion which are produced by the figure of the earth*, Washington Astronomical Papers, vol. 3 (1891), p. 213.

†Ibid., p. 340.

value the changes to be made are quite simple; the most probable value for λ is discussed elsewhere.*

From the results of my lunar theory, I find

$$\left(\frac{a^3}{3r^3}-\frac{z^2a^3}{r^5}\right)_0 = \cdots + .1287\,e^2 - 2.0060\,k^2 + .0571\,e^4 - 1.0817\,e^2k^2 + .0448\,k^4 + .0407\,e^2e'^2 - .0136\,k^2e'^2 + \cdots.$$

With $\lambda = 10^{-7} \times 3.6864$, the results, on substituting in (3), are

Characteristic.	1	e^2	k^2	e'^2	Sums.
δb_5	+ 6″.936	+ 0″.041	− 0″.118	+ 0″.001	+ 6″.860
δb_6	− 6″.400	− 0″.042	+ 0″.026	.000	− 6″.416

The values for δb_5, δb_6 differ but little from those of HILL,† + 6″.820, and − 6″.413, obtained by DELAUNAY's method with a literal expansion in powers n'/n. The terms of characteristic unity have also been obtained by using the method of my theory, and the results agree with those just found.‡

HAVERFORD COLLEGE,
February 23, 1904.

* E. W. BROWN, *On the degree of accuracy of the new lunar theory and on the final values of the mean motions of the perigee and node*, Monthly Notices of the Royal Astronomical Society, vol. 64 (1904), pp. 524–534.

† Ibid., p. 344.

‡ The complete results for the theoretical motions of the perigee and node, together with a comparison with observation, will be found in the paper *On the degree*, etc., to which reference has just been made.

SETS OF INDEPENDENT POSTULATES FOR THE ALGEBRA OF LOGIC*

BY

EDWARD V. HUNTINGTON

The algebra of symbolic logic, as developed by LEIBNIZ, BOOLE, C. S. PEIRCE, E. SCHRÖDER, and others,† is described by WHITEHEAD as "the only known member of the non-numerical genus of universal algebra."‡ This algebra, although originally studied merely as a means of handling certain problems in the logic of classes and the logic of propositions, has recently assumed some importance as an independent calculus; it may therefore be not without interest to consider it from a purely mathematical or abstract point of view, and to show how the whole algebra, in its abstract form, may be developed from a selected set of fundamental propositions, or postulates, which shall be independent of each other, and from which all the other propositions of the algebra can be deduced by purely formal processes.

In other words, we are to consider the construction of a purely *deductive theory*, without regard to its possible applications.

Introductory remarks on deductive theories in general.§ The first step in such a discussion is to decide on the *fundamental concepts* or *undefined symbols*, concerning which the statements of the algebra are to be made.

One such concept, common to every mathematical theory, is the notion of

1) a *class* (K) of *elements* $(a, b, c, \cdots)$.‖

*Presented to the Society: § 1, September 1, 1903; § 2, December 28, 1903 (and since revised); § 3 and the appendix, April 30, 1904. Received for publication, April 30, 1904.

† For an extensive bibliography, see SCHRÖDER'S *Algebra der Logik*, vol. 1 (1890).

‡ A. N. WHITEHEAD, *Universal Algebra*, vol. 1 (1898), p. 35.

§ Cf. papers by A. PADOA, cited in Transactions, vol. 4 (1903), p. 358.

‖ A *class* is determined by stating some condition which every entity in the universe must either satisfy or not satisfy; every entity which satisfies the condition is said to *belong* to the class. (If the condition is such that no entity can satisfy it, the class is called a "null" class.) Every entity which belongs to the class in question is called an *element* (cf. H. WEBER, *Algebra*, vol. 2 (1899), p. 3).

No further analysis of this concept *class*, or of similar concepts introduced below, is here attempted. For an elaborate discussion of the logical processes which underlie all mathematical thinking, see B. RUSSELL'S work on *The Principles of Mathematics*, vol. 1, 1903.

If two elements a and b are, for the purposes of the discussion in hand, *equivalent*, that is, if either may replace the other in every proposition of the algebra in question, we write $a = b$; otherwise, $a \neq b$.*

In regard to the other fundamental concepts, one has usually a considerable freedom of choice; several different sets of undefined symbols may serve as the basis of the same algebra; the only logical requirement is that the symbols of every such set must be definable in terms of the symbols of every other set. †

Thus for the algebra of logic the fundamental concepts (besides the notion of *class*) may be selected at pleasure from the following:‡

2) a *rule of combination*, § denoted, say, by $\oplus$ (read, for convenience, "plus"; see remark on these symbols below);

3) another *rule of combination*, denoted, say, by $\odot$ (read, "times");

4) a *dyadic relation*, ‖ denoted, say, by $\in$ (read, "within").

Any two of these symbols can be defined, as we shall see, in terms of the third. ¶

In the present paper, I choose the fundamental concepts as follows: In § 1;

---

* Concerning the symbol $=$ we have the following obvious theorems: 1) $a = a$, 2) if $a = b$, then $b = a$; and 3) if $a = b$ and $b = c$, then $a = c$; which are taken by many writers as the properties by which the symbol $=$ is to be defined. But cf. O. HÖLDER, *Die Axiome der Quantität und die Lehre vom Mass*, Leipziger Berichte, Math.-Phys. Classe, vol. 53 (1901), p. 4, footnote.

† Cf. remarks by M. PIERI, in his article called: *Nuovo modo di svolgere deduttivamente la geometria projettiva*, Reale Istituto Lombardo di scienze e lettere (Milano), Rendiconti, ser. 2, vol. 31 (1898), especially p. 797.

‡ For a quite different point of departure, see A. B. KEMPE, *On the relation between the logical theory of classes and the geometrical theory of points*, Proceedings of the London Mathematical Society, vol. 21, pp. 147–182, January, 1890, and *The subject-matter of exact thought*, Nature, vol. 43. pp. 156–162, December, 1890.

§ A *rule of combination* $\circ$, in the given class, is a convention according to which every two elements a and b (whether $a = b$ or $a \neq b$), in a definite order, determine uniquely an entity

$$a \circ b \text{ (read "}a \text{ with } b\text{")},$$

which is, however, not necessarily an element of the class. In the class of quantities or numbers, familiar examples of rules of combination are $+$, $-$, $\times$, $\div$, etc.

‖ A *dyadic relation*, R, in the given class, is determined when, if any two elements a and b are given in a definite order, we can decide whether a stands in the relation R to b or not; if it does, we write

$$a\mathrm{R}b, \text{ or, equally well, } b\breve{\mathrm{R}}a.$$

In the class of quantities or numbers, familiar examples of dyadic relations are $=$, $<$, $>$, $\leqq$, etc. Relationships among human beings furnish other examples. [If R is such that $a\mathrm{R}a$ for every element a, then R is called a *reflexive* relation; if R is such that $a\mathrm{R}b$ and $b\mathrm{R}c$ together always imply $a\mathrm{R}c$, then R is called a *transitive* relation; if R is such that $a\mathrm{R}b$ always implies $b\mathrm{R}a$, then R is called a *symmetric* relation. Thus the relation $\leqq$ is reflexive and transitive, but not symmetric; the relation of equivalence is reflexive, transitive and symmetric.]

¶ In all discussions like the present, *definitions* are purely *nominal definitions*, introducing a new symbol as an abbreviation for an old concept. Cf. papers by PEANO and BURALI-FORTI in Bibliothèque du congrès international de philosophie, Paris, 1900, vol. 3 (published in 1901).

the two rules of combination, $\oplus$ and $\odot$; in § 2, the relation $\circledcirc$; in § 3, a single rule of combination, $\oplus$. The three sections form properly three separate papers.

Having chosen the fundamental concepts, the next step is to decide on the *fundamental propositions*, or *postulates*, which are to stand at the basis of the algebra. These postulates are simply *conditions* arbitrarily imposed on the fundamental concepts and must not, of course, be inconsistent among themselves. Any set of *consistent* * postulates would give rise to a corresponding algebra,—namely the totality of propositions which follow from these postulates by logical deduction.† For the sake of elegance, every set of postulates should be free from redundancies; in other words, the postulates of every set should be *independent*, no one of them deducible from the rest.‡ For, if any one of the postulates were a consequence of the others, it should be counted among the derived, not among the fundamental propositions. Furthermore, each postulate should be as nearly as possible a *simple statement*, not decomposable into two or more parts; but the idea of a simple statement is a very elusive one, which has not yet been satisfactorily defined, much less attained.§

In selecting a set of consistent, independent postulates for any particular algebra, one has usually a considerable freedom of choice; several different sets of independent postulates (on a given set of fundamental concepts) may serve as the basis of the same algebra;‖ the only logical requirement is that every such set of postulates must be deducible from every other.¶

Thus, for the algebra of logic, several different sets of postulates might be given on each of the three sets of fundamental concepts which we have selected. In the present paper a single set of postulates is chosen for each of the three sections.

Object of the present paper. The object of the paper can now be stated as follows: Having chosen a set of fundamental concepts and a set of fundamental propositions for each of the three sections, I show, first, that the fundamental

* On the consistency (Widerspruchslosigkeit) of a set of postulates, see a problem of HILBERT's cited in Transactions, vol. 4 (1903), p. 361, and an article by A. PADOA, *Le problème no. 2 de M. David Hilbert*, L'Enseignement Mathématique, vol. 5 (1903), pp. 85–91.

† The processes involved in "logical deduction" have been subjected in recent years to a very searching analysis; see especially the work of G. PEANO and others in the Revue de Mathématiques, and B RUSSELL's *Principles of Mathematics*.

‡ The method of proving the independence of a postulate used and explained below, has been made familiar especially by the works of PEANO, PADOA, PIERI, and HILBERT.

§ Compare remarks by E. H. MOORE, in his paper on *A definition of abstract groups*, Transactions, vol. 3 (1902), especially pp. 488–489.

‖ For a striking example, see the postulates for a field in recent articles by L. E. DICKSON and E. V. HUNTINGTON, Transactions, vol. 4 (1903), p. 13 and p. 31.

¶ Cf. M. PIERI, *loc. cit.* Even if the postulates could be made strictly simple statements, I see no reason why several different sets of consistent, independent, and simple postulates might not be possible for the same algebra. (Cf. SCHRÖDER, *loc. cit.*, vol. 3, p. 19.)

propositions of each set are consistent (and independent); and secondly, that the fundamental concepts of each section can be defined in terms of the fundamental concepts of each of the other sections, while the fundamental propositions of each section can be deduced from the fundamental propositions of each of the other sections. Then we may say, first, that each section determines a definite algebra, and secondly, that the three algebras are equivalent.

Finally, in order to justify the name "algebra of logic" for the algebra thus established, I show that the fundamental theorems of that algebra, as set forth in standard treatises like those of SCHRÖDER and WHITEHEAD, can be derived from either of my three sections. And the development of the theory in the present paper is carried only so far as is necessary for this object.

In working out the set of postulates in § 1, I have followed WHITEHEAD closely. The postulates Ia–V are substantially the same as the fundamental propositions given in his *Universal Algebra*, Book II; except that the associative laws for addition and multiplication, which are there admitted as fundamental, are here deduced as theorems.

In § 2, postulates 1–10 are substantially the same as the fundamental positions (called by various names*) in SCHRÖDER's *Algebra der Logik;* except that postulate 9 here replaces a much less simple postulate of SCHRÖDER's which I cite for reference as 9_2. For the possibility of this simplification I am especially indebted to Mr. C. S. PEIRCE, who has kindly communicated to me a proof of the second part of the distributive law ($22a$, b) on the basis of this postulate 9. (See footnote below.) A further problem in regard to postulate 9 is proposed at the end of § 2.

The third set of postulates (§ 3) is a fairly obvious modification of the second.

The only part of the paper for which I can claim any originality (except possibly the proofs of XIIIa, b in § 1 and $20a$, b in § 2) is the establishment of the *complete independence* of all the postulates of each set. There has been no discussion of this question, as far as I know, except an only partially successful attempt of SCHRÖDER's to prove the independence of 9_2.†

A simple interpretation of the algebra. Although the algebra is necessarily treated here solely in its abstract form, without reference to its possible applications—that is, without reference to the possible interpretations of the symbols K, $\oplus$, $\odot$, and $\ominus$—nevertheless it may be well to mention at once one of the simplest of these applications, so that the reader may give a concrete interpre-

* "Prinzipien," "Postulaten," "Definitionen." See loc. cit., pp. 168, 170, 184, 188, 196, 293, 303.

† He succeeded in showing, by a very complicated method, that 9_2 is independent of postulates 1–7, omitting postulate 8. (Loc. cit., pp. 286–288, 617–628, 633–640, 642–643.) But the question whether 9_2 is independent of the full list of postulates 1–8 was left undecided; see loc. cit. p. 310, bottom.

tation, if he so desires, to all the propositions of the algebra. Any system $(K, \oplus, \odot, \oslash)$ which satisfies the postulates and definitions of § 1, § 2, or § 3 will answer the purpose. One of the simplest of such systems is the following:*

K = the class of regions in the plane including the "null region" [$= \wedge$; read "nothing"] and the whole plane [$= \vee$; read "everything"];

$a \oplus b$ = the smallest region which includes both a and b, called the "logical sum" of a and b;

$a \odot b$ = the largest region which lies within both a and b, called the "logical product" of a and b;

$\oslash$ = the relation of inclusion; that is, $a \oslash b$ signifies that the region a lies within or coincides with the region b.

Remarks on the symbols $\oplus$, $\odot$, *etc.* The symbols $\oplus$, $\odot$, and $\oslash$ are chosen with a double object in view. On account of the circles around them they are sufficiently unfamiliar to remind us of their true character as undefined symbols which have no properties not expressly stated in the postulates; while the $+$, $\cdot$, and $\prec$ within the circles enable us to adopt, with the least mental effort, the interpretation which is likely to be the most useful. The symbol $\oplus$ was used by LEIBNIZ for the same purpose about 1700.†

The symbols $\wedge$ and $\vee$, which occur below, I take from PEANO'S Formulaire de Mathématiques, vol. 4 (1903), pp. 27–28. The resemblance which these symbols bear to an empty glass and a full glass will facilitate the interpretation of them as "nothing" and "everything" respectively.

§ 1. The First Set of Postulates.

In § 1 we take as the fundamental concepts a class, K, with two rules of combination, $\oplus$ and $\odot$; and as the fundamental propositions, the following ten postulates:

I*a*. $a \oplus b$ *is in the class whenever* a *and* b *are in the class.*

I*b*. $a \odot b$ *is in the class whenever* a *and* b *are in the class.*

II*a*. *There is an element* $\wedge$ *such that* $a \oplus \wedge = a$ *for every element* a.

II*b*. *There is an element* $\vee$ *such that* $a \odot \vee = a$ *for every element* a.

III*a*. $a \oplus b = b \oplus a$ *whenever* a, b, $a \oplus b$, *and* $b \oplus a$ *are in the class.*

III*b*. $a \odot b = b \odot a$ *whenever* a, b, $a \odot b$, *and* $b \odot a$ *are in the class.*

IV*a*. $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c)$ *whenever* $a, b, c, a \oplus b, a \oplus c, b \odot c, a \oplus (b \odot c)$, *and* $(a \oplus b) \odot (a \oplus c)$ *are in the class.*

* Compare EULER'S diagrams, in works on logic.

† LEIBNIZ, *Philosophische Schriften, herausgegeben von* GERHARDT, vol. 7 (1890), p. 237; cf. Formulaire de Mathématiques, vol. 3 (1901), p. 19. On the use of the circles around these symbols, see also CHRISTINE LADD [Mrs. FRANKLIN], *On the algebra of logic*, in *Studies in Logic by members of Johns Hopkins University*, 1883, p. 18.

IV*b*. $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ *whenever* $a, b, c, a \odot b, a \odot c, b \oplus c, a \odot (b \oplus c)$ *and* $(a \odot b) \oplus (a \odot c)$ *are in the class.*

V. *If the elements* $/\!\backslash$ *and* $\backslash\!/$ *in postulates* II*a and* II*b exist and are unique, then for every element* a *there is an element* $\bar{a}$ *such that* $a \oplus \bar{a} = \backslash\!/$ *and* $a \odot \bar{a} = /\!\backslash$.

VI. *There are at least two elements,* x *and* y, *in the class such that* $x \neq y$.

Consistency of the postulates of the first set.

To show the consistency of the postulates, we have only to exhibit some system $(K, \oplus, \odot)$ in which K, $\oplus$, and $\odot$ are so interpreted that all the postulates are satisfied. For then the postulates themselves, and all their consequences, will be simply expressions of the properties of this system, and therefore cannot involve contradiction (since no system which really exists can have contradictory properties).

One such system is the following: $K =$ the class of regions in the plane including the "null region" and the whole plane; $a \oplus b =$ the "logical sum" of a and b (that is, the smallest region which includes them both); $a \odot b =$ the "logical product" of a and b (that is, the largest region which lies within them both).

Another such system, in fact the simplest possible one, is this: $K =$ a class comprising only two elements, say 0 and 1, with $\oplus$ and $\odot$ defined by the tables

$\oplus$	0	1
0	0	1
1	1	1

$\odot$	0	1
0	0	0
1	0	1

For other such systems, see the appendix.—The existence of any one of these systems is sufficient to prove the consistency of the postulates.

Deductions from the postulates of the first set.

The following theorems follow readily from the postulates I*a*–VI; the proofs are given in the next paragraph.

VII*a*. The element $/\!\backslash$ in II*a* is unique: $a \oplus /\!\backslash = a$.

VII*b*. The element $\backslash\!/$ in II*b* is unique: $a \odot \backslash\!/ = a$.

VIII*a*. $a \oplus a = a$.

VIII*b*. $a \odot a = a$.

IX*a*. $a \oplus \backslash\!/ = \backslash\!/$.

IX*b*. $a \odot /\!\backslash = /\!\backslash$.

X*a*. $a \oplus (a \odot b) = a$. (The "law of absorption.")

X*b*. $a \odot (a \oplus b) = a$.

XI. The element $\bar{a}$ in V is uniquely determined by a:

$$a \oplus \bar{a} = \bigvee \quad \text{and} \quad a \odot \bar{a} = \bigwedge.$$

DEFINITION. The element $\bar{a}$ is called non-a, or the *supplement* of a. By IIIa, IIIb, if b is the supplement of a then a is the supplement of b; that is, if $b = \bar{a}$, then $a = \bar{b}$, or, $\bar{\bar{a}} = a$.

XIIa. $a \oplus b = \overline{\bar{a} \odot \bar{b}}$, and

XIIb. $a \odot b = \overline{\bar{a} \oplus \bar{b}}$;

that is, $a \oplus b$ and $\bar{a} \odot \bar{b}$ are supplementary elements as are also $a \odot b$ and $\bar{a} \oplus \bar{b}$. These theorems establish the *principle of duality* between $\oplus$ and $\odot$, which is a characteristic feature of the algebra. They also enable us to define either multiplication or addition in terms of the other and negation.

XIIIa. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$. (Associative law for addition.)

XIIIb. $(a \odot b) \odot c = a \odot (b \odot c)$. (Associative law for multiplication.)

These theorems are sufficient to make the connection between the postulates here adopted and the usual treatment of the subject. See, for example, WHITEHEAD's *Universal Algebra*, vol. 1, book II, where two lists of fundamental propositions for the algebra of logic are given; the first list (p. 35) comprises (besides Ia, b) IIa, b, IIIa, b, IVa, V, VIIIa, b, Xa, and XIIIa, b; the second list (p. 37), which is more symmetric, includes IIa, b, IIIa, b, IVa, b, IXa, b, Xa, b, XI, and XIIIa, b.

The further development of the subject is based on the definition of $\circledcirc$, which may be given in various forms, thus,

DEFINITION. *If $a \oplus b = b$; or, if $a \odot b = a$; or, if $\bar{a} \oplus b = \bigvee$; or, if $a \odot \bar{b} = \bigwedge$; then we write $a \circledcirc b$ (or $b \circledcirc a$).*

It is easily seen that these definitions are all equivalent, and that the properties of $\circledcirc$ used as postulates in § 2 can be readily deduced.

Proofs of theorems in the preceding paragraph.

In the following proofs we write, for brevity, $a \odot b = ab$. The proofs for the theorems "b" may be obtained from the proofs for the corresponding theorems "a" by interchanging $\oplus$ with $\odot$ and $\wedge$ with $\vee$.

Proof of VIIa. Suppose there were two elements, $\bigwedge_1$ and $\bigwedge_2$, such that $a \oplus \bigwedge_1 = a$ and $a \oplus \bigwedge_2 = a$ for every element a. Then, putting $a = \bigwedge_2$ in the first equation and $a = \bigwedge_1$ in the second, we should have $\bigwedge_2 \oplus \bigwedge_1 = \bigwedge_2$ and $\bigwedge_1 \oplus \bigwedge_2 = \bigwedge_1$; whence, by III$a$, $\bigwedge_1 = \bigwedge_2$.

Proof of VIIIa. By V (in view of VIIa, b) take $\bar{a}$ so that $a \oplus \bar{a} = \bigvee$ and $a\bar{a} = \bigwedge$. Then by Ia, IIa, b, and IVa we have

$$a \oplus a = (a \oplus a) \bigvee = (a \oplus a)(a \oplus \bar{a}) = a \oplus (a\bar{a}) = a \oplus \bigwedge = a.$$

Proof of IXa. By V (in view of VIIa, b) take $\bar{a}$ so that $a \oplus \bar{a} = \vee$. Then by Ia, IIb, IIIb, and IVa we have

$$a \oplus \vee = (a \oplus \vee) \vee = \vee (a \oplus \vee) = (a \oplus \bar{a})(a \oplus \vee) = a \oplus (\bar{a} \vee) = a \oplus \bar{a} = \vee .$$

Proof of Xa. By Ia, b, IIb, IVb, IIIa, and IXa we have

$$a \oplus (ab) = (a \vee) \oplus (ab) = a(\vee \oplus b) = a(b \oplus \vee) = a \vee = a .$$

Proof of XI. Suppose that for a given element a there were two elements, $\bar{a}_1$ and $\bar{a}_2$, such that $a \oplus \bar{a}_1 = a \oplus \bar{a}_2 = \vee$ and $a\bar{a}_1 = a\bar{a}_2 = \wedge$; then using I$a$, b, IIa, b, IIIb, IVb, and V we should have

$$\bar{a}_2 = \vee \bar{a}_2 = (a \oplus \bar{a}_1)\bar{a}_2 = (a\bar{a}_2) \oplus (\bar{a}_1\bar{a}_2) = \wedge \oplus (\bar{a}_1\bar{a}_2)$$
$$= (\bar{a}_1 a) \oplus (\bar{a}_1\bar{a}_2) = \bar{a}_1(a \oplus \bar{a}_2) = \bar{a}_1 \vee = \bar{a}_1 .$$

Proof of XIIa. We notice first that

$$a \oplus (\bar{a} \oplus c) = \vee \qquad \text{and} \qquad a(\bar{a}c) = \wedge ;$$

for, by Ia, b, IIb, IIIb, IVa, V, and Xb,

$$a \oplus (\bar{a} \oplus c) = \vee [a \oplus (\bar{a} \oplus c)] = (a \oplus \bar{a})[a \oplus (\bar{a} \oplus c)]$$
$$= a \oplus [\bar{a}(\bar{a} \oplus c)] = a \oplus \bar{a} = \vee ,$$

and similarly for the reciprocal proposition.

Then, using IVa, b, IIIa, b, and XI,

$$(a \oplus b) \oplus (\bar{a}\cdot\bar{b}) = [(a \oplus b) \oplus \bar{a}]\,[(a \oplus b) \oplus \bar{b}] = \vee \vee = \vee ,$$

and

$$(a \oplus b)(\bar{a}\cdot\bar{b}) = [a(\bar{a}\cdot\bar{b})] \oplus [b(\bar{a}\cdot\bar{b})] = \wedge \cdot \wedge = \wedge ,$$

whence, by XI, $a \oplus b$ and $\bar{a}\cdot\bar{b}$ are supplementary elements.

Proof of XIIIa. Let $(a \oplus b) \oplus c = x$ and $a \oplus (b \oplus c) = y$; then $(\bar{a}\cdot\bar{b})\bar{c} = \bar{x}$, by XII$a$, and in order to prove that $x = y$ it is sufficient (by XI) to show that $\bar{x}$ and y are supplementary elements.

Now

(1) $$y \oplus \bar{a} = y \oplus \bar{b} = y \oplus \bar{c} = \vee .$$

For, first, $y \oplus \bar{a} = \bar{a} \oplus [a \oplus (b \oplus c)] = \vee$ as in the proof of XIIa; secondly,

$$y \oplus \bar{b} = \vee (\bar{b} \oplus y) = (\bar{b} \oplus b)(\bar{b} \oplus y) = \bar{b} \oplus (by) \text{ by IV}a,$$

while

$$by = b[a \oplus (b \oplus c)] = (ba) \oplus [b(b \oplus c)] = (ba) \oplus b = b, \text{ by IV}b \text{ and X}a, b,$$

so that $y \oplus \bar{b} = \bar{b} \oplus b = \vee$; and similarly, $y \oplus \bar{c} = \vee$.

Also, by a similar method,

(2) $$\bar{x}a = \bar{x}b = \bar{x}c = \wedge .$$

Therefore, by IVa,

$$y \oplus \bar{x} = y \oplus [(\bar{a}\cdot\bar{b})\bar{c}] = [(y \oplus \bar{a})(y \oplus \bar{b})](y \oplus \bar{c}) = (\vee\vee)\vee = \vee,$$

and, by IVb,

$$\bar{x}y = \bar{x}[a \oplus (b \oplus c)] = (\bar{x}a) \oplus [(\bar{x}b) \oplus (\bar{x}c)] = \wedge \oplus (\wedge \oplus \wedge) = \wedge ;$$

whence, by XI, $\bar{x}$ and y are supplementary elements. Therefore $x = y$.

Theorem XIIIb follows at once from XIIIa by XIIa, b.

Independence of the postulates of the first set.

The ten postulates of the first set are *independent;* that is, no one of them can be deduced from the other nine. To show this, we exhibit, in the case of each postulate, a system $(K, \oplus, \odot)$ which satisfies all the other postulates, but not the one in question. This postulate, then, cannot be a consequence of the others; for if it were, every system which had the other properties would have this property also, which is not the case.

For postulate VI take $K =$ the class comprising a single element, a, with $a \oplus a = a$ and $a \odot a = a$.

For the other postulates, take $K =$ a class containing two elements, say 0 and 1, with $\oplus$ and $\odot$ defined appropriately for each case, as indicated in the following scheme:

	$0 \oplus 0$	$0 \oplus 1$	$1 \oplus 0$	$1 \oplus 1$	$0 \odot 0$	$0 \odot 1$	$1 \odot 0$	$1 \odot 1$
Ia)	0	1	1	x	0	0	0	1
Ib)	0	1	1	1	x	0	0	1
IIa)	0	0	0	0	0	0	0	1
IIb)	0	1	1	1	1	1	1	1
IIIa)	0	0	1	1	0	0	0	1
IIIb)	0	1	1	1	0	0	1	1
IVa)	0	1	1	0	0	0	0	1
IVb)	0	1	1	1	1	0	0	1
V)	0	1	1	1	0	1	1	1

In verifying these results, notice that the system for IIa (or IIb) satisfies postulate V "vacuously," since no element having the properties of $\wedge$ (or $\vee$) exists; while the system for IIIa (or IIIb) also satisfies V vacuously, since the element $\wedge$ (or $\vee$) is not uniquely determined. In the other systems, $\wedge = 0$ and $\vee = 1$, except in the system for V, where $\wedge = 0$ and $\vee = 0$.

§ 2. The Second Set of Postulates.

In § 2 we take as the fundamental concepts a class, K, with a dyadic relation, $\odot$; and as the fundamental propositions, the following ten postulates. (Note that $a \odot b$ and $b \odot a$ mean the same thing.)

1. *$a \odot a$ whenever a belongs to the class.*
2. *If $a \odot b$ and also $a \odot b$, then $a = b$.*
3. *If $a \odot b$ and $b \odot c$, then $a \odot c$.*
4. *There is an element $/\!\backslash$ such that $/\!\backslash \odot a$ for every element $a \neq /\!\backslash$.*
5. *There is an element $\backslash\!/$ such that $\backslash\!/ \odot a$ for every element $a \neq \backslash\!/$.*
6. *If $a \neq b$, and neither $a \odot b$ nor $a \odot b$, there is an element s such that*

   1°) $s \odot a$; 2°) $s \odot b$; *and*

   3°) *if $y, \neq s$, is such that $y \odot a$ and $y \odot b$, then $y \odot s$.*
7. *If $a \neq b$, and neither $a \odot b$ nor $a \odot b$, there is an element p such that*

   1°) $p \odot a$; 2°) $p \odot b$; *and*

   3°) *if $x, \neq p$, is such that $x \odot a$ and $x \odot b$, then $x \odot p$.*
8. *If the elements $/\!\backslash$ and $\backslash\!/$ in 4 and 5 exist and are unique, then for every element a there is an element $\bar{a}$ such that*

   1°) *if $x \odot a$ and $x \odot \bar{a}$, then $x = /\!\backslash$; and*

   2°) *if $y \odot a$ and $y \odot \bar{a}$, then $y = \backslash\!/$.*
9. *If postulates 1, 4, 5, and 8 hold, and if $a \odot \bar{b}$ is false, then there is an element $x \neq /\!\backslash$ such that $x \odot a$ and $x \odot b$.*
10. *There are at least two elements, x and y, such that $x \neq y$.*

In this list, postulates 1–7 are independent among themselves, and postulates 8 and 9 are independent of the first seven (ordinally independent). Taking the whole list together, however, either 6 or 7 can be deduced from the rest, as shown in 25 below. Both postulates 6 and 7 are allowed to stand in the list for reasons of symmetry; but if a set of absolutely (not merely ordinally) independent postulates is desired, either one or the other must be omitted.

Consistency of the postulates of the second set.

To show the consistency of the postulates, we have only to exhibit some system $(K, \odot)$ in which K and $\odot$ are so interpreted that all the postulates are satisfied.

One such system is the following: $K =$ the class of regions in the plane (including the null-region and the whole plane); $a \odot b$ signifying that the region a lies within (or coincides with) the region b.

Another such system is the class composed of two elements, 0 and 1 with $0 \odot 0$, $0 \odot 1$, and $1 \odot 1$, but not $1 \odot 0$.

For other such systems, see the appendix.

Deductions from the postulates of the second set.

The following theorems are deduced from the postulates of the second set, and are sufficient to connect these postulates with the usual presentation of the theory; the proofs wherever needed are given in the next paragraph. The postulates on which each theorem depends are indicated at the right.

11*a*. The element $\wedge$ in 4 is unique. (2, 4)

Hence $\wedge \odot a$ for every element a; and if $x \odot \wedge$, then $x = \wedge$. (1, 2, 4)

11*b*. The element $\vee$ in 5 is unique. (2, 5)

Hence $\vee \odot a$ for every element a; and if $y \odot \vee$, then $y = \vee$. (1, 2, 4)

12*a*. The element s in 6 is uniquely determined by a and b; hence we may define $a \oplus b$ as follows:

DEFINITION. If $a \odot b$, $a \oplus b = b$; if $a \odot b$, $a \oplus b = a$; if $a = b$, $a \oplus a = a$; otherwise, $a \oplus b = s$ (in 6). Hence $a \oplus b \odot a$ and $a \oplus b \odot b$; and if $y \odot a$ and $y \odot b$, then $y \odot a \oplus b$. Obviously, $a \oplus b = b \oplus a$. (1, 2, 6)

12*b*. The element p in 7 is uniquely determined by a and b; hence we may define $a \odot b$, or ab, as follows:

DEFINITION. If $a \odot b$, $ab = a$; if $a \odot b$, $ab = b$; if $a = b$, $aa = a$; otherwise, $ab = p$ (in 7). Hence $ab \odot a$ and $ab \odot b$; and if $x \odot a$ and $x \odot b$ then $x \odot ab$. Obviously $ab = ba$. (1, 2, 7)

13*a*. $a \oplus \wedge = a$ and $a \oplus \vee = \vee$. (1, 2, 4, 5, 6)

13*b*. $a \vee = a$ and $a \wedge = \wedge$. (1, 2, 4, 5, 7)

14*a*. If $y \odot a \oplus b$, then $y \odot a$ and $y \odot b$. (1, 2, 3, 6)

14*b*. If $x \odot ab$, then $x \odot a$ and $x \odot b$. (1, 2, 3, 7)

15*a*. If $a \odot b$ and $x \odot y$, then $a \oplus x \odot b \oplus y$. (1, 2, 3, 6)

In particular, if $x \odot y$, then $a \oplus x \odot a \oplus y$.

15*b*. If $a \odot b$ and $x \odot y$, then $ax \odot by$. (1, 2, 3, 7)

In particular, if $x \odot y$, then $ax \odot ay$.

16*a*. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$. (1, 2, 3, 6)

16*b*. $(ab)c = a(bc)$. (1, 2, 3, 7)

17. The element $\bar{a}$ in 8 is uniquely determined by a; hence

DEFINITION. *The element* $\bar{a}$ *(in* 8*) is called non-*a*, or the supplement of* a. Hence, $a \oplus \bar{a} = \vee$ and $a\bar{a} = \wedge$. Obviously, $\bar{\wedge} = \vee$ and $\bar{\vee} = \wedge$. (1, 2, 4, 5, 8, 9)

18. If $\bar{a} = b$, then $a = \bar{b}$; hence, $\bar{\bar{a}} = a$, by 17. (1, 2, 4, 5, 8, 9)

19. If $a \odot b$ then, inversely, $\bar{b} \odot \bar{a}$. (1, 2, 3, 4, 5, 8, 9)

$20a.\ a \oplus b = \overline{\bar{a} \odot \bar{b}}.$ (1, 2, 3, 4, 5, 6, 7, 8, 9)

$20b.\ a \odot b = \overline{\bar{a} \oplus \bar{b}}.$ (1, 2, 3, 4, 5, 6, 7, 8, 9)

These last theorems, $20a$ and $20b$, establish the duality between $a \oplus b$ and $a \odot b$.

$21a.\ a(b \oplus c) \supset ab \oplus ac.$ (1, 2, 3, 6, 7)

$21b.\ a \oplus bc \subset (a \oplus b)(a \oplus c).$ (1, 2, 3, 6, 7)

$22a.\ a(b \oplus c) \subset ab \oplus ac.$ (1, 2, 3, 4, 5, 6, 7, 8, 9)

$22b.\ a \oplus bc \supset (a \oplus b)(a \oplus c).$ (1, 2, 3, 4, 5, 6, 7, 8, 9)

From theorems 21 and 22 the distributive laws follow at once, by 2, namely,

$23a.\ a(b \oplus c) = ab \oplus ac.$ (1, 2, 3, 4, 5, 6, 7, 8, 9)

$23b.\ a \oplus bc = (a \oplus b)(a \oplus c).$ (1, 2, 3, 4, 5, 6, 7, 8, 9)

All these theorems would hold for a class containing only a single element a, with $a \subset a$. This trivial case is excluded by postulate 10, however, and we have:

24. $\bar{a} \neq a$; in particular, $\wedge \neq \vee$. (1, 2, 4, 5, 6, 7, 8, 10)

$25a$. Postulate 6 is a consequence of postulates 1, 2, 3, 4, 5, 7, 8, and 9; the required element s being $s = \overline{\bar{a} \odot \bar{b}}$.

$25b$. Postulate 7 is a consequence of postulates 1, 2, 3, 4, 5, 6, 8, and 9; the required element p being $p = \overline{\bar{a} \oplus \bar{b}}$.

Proofs of theorems in the preceding paragraph.

The theorems $11a, b$ and $12a, b$ follow immediately from the postulates indicated. In theorems $13a, b$ it is sufficient to notice that the sum or product given has the properties stated in $12a, b$. Theorems $14a$ and $14b$ follow from $12a$ and $12b$ by 3. The remaining theorems may be proved as follows, the proof for any theorem "b" being in each case readily supplied from the proof for the corresponding theorem "a" by interchanging $\subset$ with $\supset$, $\oplus$ with $\odot$, and $\wedge$ with $\vee$.*

Proof of $15a$. By $12a$, $a \oplus x \supset a$ and $a \oplus x \supset x$. From $a \oplus x \supset a$ and $a \supset b$, by 3, $a \oplus x \supset b$; from $a \oplus x \supset x$ and $x \supset y$, by 3, $a \oplus x \supset y$; therefore, by $12a$, $a \oplus x \supset b \oplus y$.

Proof of $16a$. By $12a$, $(a \oplus b) \oplus c \supset a \oplus b$, and $a \oplus b \supset a$; hence, by 3, $(a \oplus b) \oplus c \supset a$. But also, $a \oplus b \supset b$, whence $(a \oplus b) \oplus c \supset b$; and further, $(a \oplus b) \oplus c \supset c$, by $12a$; hence, by $12a$, $(a \oplus b) \oplus c \supset (b \oplus c)$. Therefore, by $12a$, $(a \oplus b) \oplus c \supset a \oplus (b \oplus c)$.

Similarly, $a \oplus (b \oplus c) \supset (a \oplus b) \oplus c$. Hence the theorem, by 2.

* Theorems $21b$, $22b$, and $23b$ may also be inferred directly from $21a$, $22a$, and $23a$, by the aid of the principle of duality established in $20a$ and $20b$.

Proof of 17. Let $\bar{a}_1$ and $\bar{a}_2$ be two elements having the properties of $\bar{a}$ in 8.

Then $\bar{a}_1 \odot \bar{a}_2$; for if not, we should have, by 9, an element $x \neq \wedge$ such that $x \odot \bar{a}_1$ and $x \odot a$, whence, by 8 and 11a, $x = \wedge$.

Again, $\bar{a}_2 \odot \bar{a}_1$; for, if not, we should have, by 9, an element $y \neq \wedge$ such that $y \odot \bar{a}_2$ and $y \odot a$, whence, by 8 and 11a, $y = \wedge$.

Therefore $\bar{a}_1 = \bar{a}_2$, by 2.

Proof of 18. From $\bar{a} = b$ we have: if $x \odot a$ and $x \odot b$, then $x = \wedge$; and if $y \oplus a$ and $y \oplus b$, then $y = \vee$. But these are precisely the conditions under which $a = \bar{b}$, by 8.

Proof of 19. If $\bar{b} \odot \bar{a}$ were false, we should have, by 9, an element $x \neq \wedge$ such that $x \odot \bar{b}$ and $x \odot a$. But from $x \odot a$ and $a \odot b$ follows $x \odot b$, by 3; and from $x \odot b$ and $x \odot \bar{b}$ follows $x = \wedge$, by 8 and 11a, which contradicts the condition $x \neq \wedge$.

Proof of 20a. Let $a \oplus b = s$ and $\bar{a}\cdot\bar{b} = \bar{p}$; it is required to prove (see 18) that $s = p$.

By 12a, $s \oplus a$ and $s \oplus b$; hence by 19, $\bar{s} \odot \bar{a}$ and $\bar{s} \odot \bar{b}$, or, by 12b, $\bar{s} \odot \bar{a}\cdot\bar{b}$; that is $\bar{s} \odot \bar{p}$, or by 19, $p \odot s$.

Again, by 12b, $\bar{p} \odot \bar{a}$ and $\bar{p} \odot \bar{b}$; hence, by 19, $p \oplus a$ and $p \oplus b$, or, by 12a, $p \oplus a \oplus b$; that is, $p \oplus s$.

Therefore $s = p$, by 2.

Proof of 21a. By 12b, $ab \odot a$ and $ac \odot a$, whence, by 12a,

$$ab \oplus ac \odot a.$$

Again, $ab \odot b$ and $ac \odot c$, by 12b; hence, by 15a,

$$ab \oplus ac \odot b \oplus c.$$

Therefore, $ab \oplus ac \odot a(b \oplus c)$, by 12$b$.

Proof of 22a.* In order to facilitate the proof of this theorem, we first establish the following

LEMMA: $a(b \oplus c) \odot b \oplus ac$.

---

*This demonstration is borrowed, almost verbatim, from a letter of Mr. C. S. PEIRCE'S, dated December 24, 1903. Mr. PEIRCE uses the symbol $\prec$ where I have used $\odot$, and in a slightly different sense; so that he is enabled to state that the principle here called postulate 9 "follows from the definition of $P_i \prec C_i$ on page 18" of his article of 1880. The demonstration was originally worked out for that article (American Journal of Mathematics, vol. 3 (1880), p. 33), but is now published for the first time (compare *ibid.*, vol. 7, p. 190, footnote, 1885 [wrongly cited as 1884 in SCHRÖDER'S bibliography], and SCHRÖDER, *loc. cit.*, p. 291).

Under the date February 14, 1904, Mr. PEIRCE writes as follows:

"Dear Mr. HUNTINGTON: Should you decide to print the proof of the distributive principle (and this would not only relieve me from a long procrastinated duty, but would have a certain value for exact logic, as removing the eclipse under which the method of developing the subject followed in my paper in vol. 3 of the American Journal of Mathematics has been obscured) I should feel that it was incumbent upon me, in decency, to explain its having been so long withheld. The truth is that the paper aforesaid was written during leisure hours gained to me by

Suppose the lemma to be false. Then, by 9 and 18, there is an element $x \neq /\!\backslash$ such that

$$x \circledcirc a(b \oplus c), \tag{1°}$$

and $$x \circledcirc \overline{b \oplus ac},$$

whence, by 19, $$\bar{x} \circledcirc b \oplus ac. \tag{2°}$$

From (1°), by 14*b*, $$x \circledcirc a, \tag{3°}$$

and $$x \circledcirc b \oplus c. \tag{4°}$$

From (2°), by 14*a*, $\bar{x} \circledcirc b$ and $\bar{x} \circledcirc ac$, whence, by 19,

$$x \circledcirc \bar{b}, \tag{5°}$$

and $$x \circledcirc \overline{ac}. \tag{6°}$$

From (6°) and (3°) it follows that $x \circledcirc c$ must be false: for if $x \circledcirc c$ and $x \circledcirc a$, then $x \circledcirc ac$ by 12*b*, whence $x = /\!\backslash$, by 17, which contradicts the condition $x \neq /\!\backslash$.

Therefore, by 9 and 18, there is an element $y \neq /\!\backslash$ such that

$$y \circledcirc x, \tag{7°}$$

and $$y \circledcirc \bar{c},$$

whence, by 19, $$\bar{y} \circledcirc c. \tag{8°}$$

From (7°) and (5°), by 3, $y \circledcirc \bar{b}$, whence by 19,

$$\bar{y} \circledcirc b. \tag{9°}$$

From (8°) and (9°) by 12*a*, $\bar{y} \circledcirc b \oplus c$, whence, by 19,

$$y \circledcirc \overline{b \oplus c}. \tag{10°}$$

But from (7°) and (4°), by 3, we have

$$y \circledcirc b \oplus c, \tag{11°}$$

and from (10°) and (11°), by 17, $y = /\!\backslash$, which contradicts the condition $y \neq /\!\backslash$.

---

my being shut up with a severe influenza. In writing it, I omitted the proof, as there said, because it was 'too tedious' and because it seemed to me very obvious. Nevertheless, when Dr. SCHRÖDER questioned its possibility, I found myself unable to reproduce it, and so concluded that it was to be added to the list of blunders, due to the grippe, with which that paper abounds, —a conclusion that was strengthened when SCHRÖDER thought he demonstrated the indemonstrability of the law of distributiveness. (I must confess that I never carefully examined his proof, having my table loaded with logical books for the perusal of which life was not long enough.) It was not until many years afterwards that, looking over my papers of 1880 for a different purpose, I stumbled upon this proof written out in full for the press, though it was eventually cut out, and, at first, I was inclined to think that it employed the principle that *all* existence is individual, which my method, in the paper in question, did not permit me to employ at that stage. I venture to opine that it fully vindicates my characterization of it as 'tedious.' But this is how I have a new apology to make to exact logicians."

Therefore the supposition from which we started is impossible, and the lemma is established.

The proof of the main theorem then proceeds as follows: By the lemma,

$$a(b \oplus c) \odot b \oplus ac.$$

Therefore, by 15b, $\quad a[a(b \oplus c)] \odot a[b \oplus ac]. \qquad (12°)$

But, by 16b and 12b,

$$a[a(b \oplus c)] = (aa)(b \oplus c) = a(b \oplus c), \qquad (13°)$$

and by 12a and the lemma again,

$$a[b \oplus ac] = a(ac \oplus b) \odot ac \oplus ab = ab \oplus ac. \qquad (14°)$$

Therefore, by 3,

$$a(b \oplus c) \odot ab \oplus ac.$$

Proof of 23a. This theorem follows at once from 21a and 22a by 2.

Proof of 24. If $\bar{a} = a$ for any particular element a, then $a = \wedge$, by 8, 1, and 11a. But if $\overline{\wedge} = \wedge$, then $\wedge = \vee$, by 8, 1, and 11b; whence, every element coincides with $\wedge$, by 2—a result which is impossible by 10. Therefore $\bar{a} \neq a$, for every element a.

Proof of 25a. Let $s = \overline{\bar{a} \odot \bar{b}}$; we have then to show that this element s has the properties 1°), 2°), and 3°) demanded by postulate 6. By 18 and 12b, $\bar{a} \odot \bar{b} \odot \bar{a}$ and $\bar{a} \odot \bar{b} \odot \bar{b}$; hence, by 19, $s \odot a$ and $s \odot b$. Further, if $y \odot a$ and $y \odot b$, then, by 19, $\bar{y} \odot \bar{a}$ and $\bar{y} \odot \bar{b}$; whence, by 12b, $\bar{y} \odot \bar{a} \odot \bar{b}$, or, by 19, $y \odot s$.

Independence of the postulates of the second set.

The independence of the nine postulates of the second set (either 6 or 7 being omitted) is shown by the following systems $(K, \odot)$, each of which satisfies all the other postulates, but not the one for which it is numbered.

(1) K = a class of four elements, say 0, 1, 2, 3, with $\odot$ defined by the accompanying "relation table." In a table of this kind,* a dot standing to

$\odot$	2	0	1	3
2	•		•	
0	•		•	•
1				
3			•	•

*SCHRÖDER makes extensive use of tables of this kind in his *Algebra der Logik;* see vol. 3 (1895), p. 44.

the right of a and underneath b indicates that the relation $a \circledcirc b$ is true; the absence of such a dot indicates that $a \circledcirc b$ is false. Here postulate 1 is not satisfied, for $0 \circledcirc 0$ and $1 \circledcirc 1$ are not true. In postulates 4 and 5, take $/\!\backslash = 0$ and $\backslash/ = 1$. In postulate 8, take $\bar{0} = 1$, $\bar{\bar{2}} = 3$, and conversely. Postulate 9 is satisfied vacuously.

(2) $K =$ a class of two elements, α and β, with $\circledcirc$ interpreted as "equal to or different from," so that $a \circledcirc b$ is always true.

Here postulate 2 is clearly false. Postulate 9 is satisfied vacuously, since $a \circledcirc \bar{b}$ is never false.

(3) $K =$ a class of six elements, $0, 1, 2, \cdots, 5$, with $\circledcirc$ defined as in the accompanying table.

$\circledcirc$	4	2	0	1	3	5
4	•			•	•	
2	•	•		•		
0	•	•	•	•	•	•
1				•		
3				•	•	•
5		•		•		•

Here postulate 3 is false, since $2 \circledcirc 4$ and $4 \circledcirc 3$, but not $2 \circledcirc 3$. In postulates 4 and 5, take $/\!\backslash = 0$, $\backslash/ = 1$. In postulate 8, take $\bar{0} = 1$, $\bar{\bar{2}} = 3$, $\bar{\bar{4}} = 5$, and conversely.

(4) $K =$ the class of all the finite sets of integers which include the integer 1; with $\circledcirc$ interpreted as "the same as or includes." (Thus, $a \circledcirc b$ means that every integer in the set b is also in the set a.)

Postulate 4 fails, since there is no set which includes all the other sets. In 5, take $\backslash/ = 1$. In 6 and 7, let s be the set of integers common to the sets a and b, and p the sets composed of a and b together. Postulates 8 and 9 are satisfied vacuously.

(5) $K =$ the class of all the finite sets of integers which include the integer 0; with $\circledcirc$ interpreted as "the same as or part of." (Thus, $a \circledcirc b$ means that every integer in the set a is also in the set b.)

Postulate 5 fails, since there is no set of which every other set is a part. In 4, take $/\!\backslash = 0$. In 6 and 7, let s be the set composed of sets a and b together, and p the set of integers common to the sets a and b.

(6 *and* 7). $K =$ a class of fourteen elements, denoted, say, by u_0; $u_{01}, u_{02}, u_{03}, u_{04}$; $u_{012}, u_{013}, u_{024}, u_{034}$; $u_{0123}, u_{0124}, u_{0134}, u_{0234}$; u_{01234}; with $\circledcirc$ defined as follows: $u_A \circledcirc u_B$ when and only when the digits in the subscript A are all included among the digits in the subscript B. (Notice that u_{014} and u_{023} are not included in the class.)

Here postulates 1–5 clearly hold. Postulate 6 fails when $a = u_{01}$, $b = u_{04}$, and also when $a = u_{02}$, $b = u_{03}$. Postulate 7 fails when $a = u_{0124}$, $b = u_{0134}$, and also when $a = u_{0123}$, $b = u_{0234}$. Postulates 8 and 9 hold.

(8) K = a class of three elements, 0, 1, 2, with $\odot$ defined by the accompanying table.

$\odot$	0	2	1
0	•	•	•
2		•	•
1			•

Here postulates 4 and 5 hold, and $\wedge$ and $\vee$ are unique: $\wedge = 0$, $\vee = 1$ But postulate 8 is false for the case $a = 2$.

(9) K = a class of five elements, 0, 1, 2, 3, 4, with $\odot$ defined by the accompanying table.

$\odot$	0	2	3	4	1
0	•	•	•	•	•
2		•		•	•
3			•		•
4				•	•
1					•

Here postulates 4 and 5 are satisfied: $\wedge = 0$, $\vee = 1$; and also postulate 8, although the element $\bar{a}$ is not always uniquely determined by a: thus, $\bar{0} = 1$, $\bar{2} = 3$, $\bar{3} = 2$ or 4, $\bar{4} = 3$, $\bar{1} = 0$. Postulates 9 fails, since $4 \odot 2$ is false, while $x = 0$ is the only element x such that $x \odot 4$ and $x \odot 3$.

I have not been able to find a system for (9) in which $\bar{a}$ is always uniquely determined by a; see the unsolved problem proposed below.

(10) K = a class comprising a single element a, with $a \odot a$. (Postulate 9 is satisfied vacuously.)

Thus the postulates of § 2, *omitting either* 6 *or* 7, are independent, as was to be proved.

It is interesting to notice also that, if we confine ourselves to the first seven postulates, then postulates 6 and 7 are independent of each other. This is proved by the following systems, each of which satisfies all the postulates 1–7 except the one for which it is numbered.

(6) K = a class composed of the following areas: all the squares which lie within a given square (with sides parallel to the sides of the given square); the given square itself, and the "null" square; a fixed circle, lying wholly within the given square; and all areas formed by the addition of two or more of these areas;—with $\odot$ interpreted as "includes or coincides with."

Postulates 1–5 clearly hold. (In 4, $\wedge$ = the whole square; in 5, $\vee$ = the null-square). Postulate 6 fails when a = the circle and b = a square which overlaps the circle; for there is no *largest* area (belonging to the class) which lies within both a and b. Postulate 7 holds, the area p being the combined area of a and b.

(7) K = the same class as used above in the proof of the independence of 6; with $\Subset$ interpreted as "within or coincident with."

Postulates 1–5 clearly hold. (In 4, $\curlywedge$ = the null-square; in 5, $\vee$ = the whole square). Postulate 6 holds, the area s being the combined area of a and b. Postulate 7 fails when a = the circle and b = a square which overlaps the circle; for there is no *largest* area (belonging to the class) which lies within both a and b.

A problem connected with postulate 9.

Other forms which may be used in place of postulate 9 are the following [assuming such of the postulates 1–8 as may be necessary, and defining $a \oplus b$ and $a \odot b (= ab)$ as above]:

9_1. If $bc = \curlywedge$, then $b \Subset \bar{c}$.

9_2.* If $bc = \curlywedge$, then $a(b \oplus c) \Subset ab \oplus ac$ [whence $a(b \oplus c) = ab \oplus ac$, by 2 and $21a$].

9_3.† $a \Subset ab \oplus a\bar{b}$ [whence $a = ab \oplus a\bar{b}$, by 2 and $21a$].

The form 9_1 can be deduced from 9_2 or 9_3 as follows: if $bc = \curlywedge$, then $b\bar{c} = bc \oplus b\bar{c} = b(c \oplus \bar{c}) = b \vee = b$; whence, $b \Subset \bar{c}$.

The form 9 can be deduced from 9_1 as follows: if $a \Subset \bar{b}$ is false, there must be some element $x \neq \curlywedge$, such that $x \Subset a$ and $x \Subset b$; for, if there were no element except $\curlywedge$ which is $\Subset a$ and $\Subset b$, then by $12b$, $ab = \curlywedge$, whence, by 9_1, $a \Subset \bar{b}$, which contradicts the hypothesis.

The form 9_1 is clearly simpler than 9_2 or even than 9_3; but all these forms are in so far unsatisfactory as they lack the symmetry which corresponds to the principle of duality between $\oplus$ and $\odot$.

I therefore propose the following problem: *if postulate* 9 *is replaced by* 9_4, *namely:*

> 9_4. If the elements $\curlywedge$ and $\vee$ in postulates 4 and 5 exist and are unique, and if postulates 8 is true, then the element $\bar{a}$ in 8 is uniquely determined by the element a;

can 9 *then be deduced from* 9_4, *or must some other postulate be added?*

In this connection, 19 is clearly of special importance.

* This is SCHRÖDER'S "Prinzip $\mathrm{III}_\times$" (*loc. cit.*, p. 293), from which he showed that the distributive law, 23, can be deduced.

† This is SCHRÖDER'S "Prinzip $\mathrm{III}^0_\times$," a weaker form of his "Prinzip $\mathrm{III}_\times$," and not, as far as he could see without the knowledge of a proof like that of PEIRCE'S in the present paper, sufficient for his purpose.

§ 3. The Third Set of Postulates.

In § 3 we take as the fundamental concepts a class, K, with a rule of combination, $\oplus$; and as the fundamental propositions, the following nine postulates:

A. $a \oplus a = a$ *whenever* a *and* $a \oplus a$ *belong to the class.*

B. $a \oplus b = b \oplus a$ *whenever* a, b, $a \oplus b$, *and* $b \oplus a$ *belong to the class.*

C. $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ *whenever* a, b, c, $a \oplus b$, $b \oplus c$, $(a \oplus b) \oplus c$, *and* $a \oplus (b \oplus c)$ *belong to the class.*

D. There is an element $/\!\backslash$ *such that* $a \oplus /\!\backslash = a$ *for every element* a.

E. There is an element $\backslash\!/$ *such that* $\backslash\!/ \oplus a = \backslash\!/$ *for every element* a.

F. If a *and* b *belong to the class, then* $a \oplus b$ *belongs to the class.*

G. If the elements $/\!\backslash$ *and* $\backslash\!/$ *in postulates D and E exist and are unique, then for every element* a *there is an element* $\bar{a}$ *such that*

$$1°) \text{ if } x \oplus a = a \text{ and } x \oplus \bar{a} = \bar{a}, \text{ then } x = /\!\backslash;$$

$$\text{and} \qquad 2°) \; a \oplus \bar{a} = \backslash\!/ .$$

H. If postulates A, D, E, *and* G *hold, and if* $a \oplus \bar{b} \neq \bar{b}$ *then there is an element* $x \neq /\!\backslash$ *such that* $a \oplus x = a$ *and* $b \oplus x = b$.

J. There are at least two elements, x *and* y, *such that* $x \neq y$.

Consistency of the postulates of the third set.

The consistency of the postulates is shown by the existence of the following system $(K, \oplus)$, in which all the postulates are satisfied:

$K =$ the class of regions in the plane (including the null region and the whole plane); $a \oplus b =$ the "logical sum" of the regions a and b, that is, the smallest region which includes them both.

Another such system is the class composed of two elements, 0 and 1, with $\oplus$ defined by the table

$\oplus$	0	1
0	0	1
1	1	1

For other such systems, see the appendix.

Deductions from the postulates of the third set.

All the postulates of § 2 are very easily deduced from the postulates of § 3 when $\odot$ is defined as follows:

DEFINITION. We shall write $a \circledcirc b$ (or $b \circledcirc a$) when and only when $a \oplus b = b$.

The proof of 6, for example, is as follows: By F, B, C and A,

$$(a \oplus b) \oplus a = a \oplus (a \oplus b) = (a \oplus a) \oplus b = a \oplus b,$$

and similarly $(a \oplus b) \oplus b = a \oplus b$; whence, $a \oplus b \circledcirc a$ and $a \oplus b \circledcirc b$. Further, if $y \circledcirc a$ and $y \circledcirc b$, then $a \oplus y = y$ and $b \oplus y = y$, whence $(a \oplus y) \oplus (b \oplus y) = y \oplus y$, or $(a \oplus b) \oplus y = y$, or $y \circledcirc (a \oplus b)$.

Postulate 7 follows as in $25b$, and we may define $a \odot b$ thus:

DEFINITION. $a \odot b = \bar{a} \oplus \bar{b}$.

The equivalence between the algebra of § 3 and the algebras of § 1 and § 2 is thus readily established.

Independence of the postulates of the third set.

The independence of the nine postulates of the third set is shown by the following systems $(K, \oplus)$, each of which satisfies all the other postulates, but not the one for which it is lettered.

(A) The class of positive integers, and 0 and ∞; with $a \oplus b = a + b$.

Here postulates B–F clearly hold. In G take $\bar{a} = \infty$ when $a \neq \infty$, and $\bar{a} =$ any other element when $a = \infty$. Postulate H is satisfied vacuously.

(B) A class of two or more elements, with $a \oplus b = a$.

Here B clearly fails. In D, E, and F, any elements will answer as $\wedge$ and $\vee$. Postulate G is satisfied vacuously, since $\wedge$ and $\vee$ are not uniquely determined. In H, $x =$ any element.

(C) A class of six elements, $0, 1, 2, \cdots, 5$, with $\oplus$ defined as in the accompanying table.

$\oplus$	4	2	0	1	3	5
4	4	4	4	1	3	1
2	4	2	2	1	1	2
0	4	2	0	1	3	5
1	1	1	1	1	1	1
3	3	1	3	1	3	5
5	1	2	5	1	5	5

Here C fails, since $(2 \oplus 4) \oplus 3 = 4 \oplus 3 = 3$, while $2 \oplus (4 \oplus 3) = 2 \oplus 3 = 1$. In D and E, take $\wedge = 0$ and $\vee = 1$. Postulate G holds: $\bar{0}=1$, $\bar{2}=3$, $\bar{4}=5$, and conversely. Postulate H also holds.

(D) The class of all the finite sets of integers which include the integer 1; with $a \oplus b$ defined as the set of integers common to the sets a and b.

Here D fails, since no set includes all the rest. In E, take $\vee = 1$. Postulates G and H are satisfied vacuously.

(E) The class of all the finite sets of integers which include the integer 0; with $a \oplus b$ defined as the set composed of the sets a and b together.

Here E fails, since no set includes all the rest. In D, take $\wedge = 0$. Postulates G and H are satisfied vacuously.

(F) The class of fourteen elements used in proving the independence of 6 and 7 in § 2; with $\oplus$ defined as follows: $u_A \oplus u_B = u_S$, where the subscript S includes all the digits in the subscript A and also all those in the subscript B.

Here F fails when $a = u_{01}$, $b = u_{04}$, and also when $a = u_{02}$, $b = u_{03}$.

(G) A class of three elements, 0, 1, 2, with $\oplus$ defined as in the accompanying table.

$\oplus$	0	2	1
0	0	2	1
2	2	2	1
1	1	1	1

Here G fails when $a = 2$. In D and E, take $\wedge = 0$ and $\vee = 1$. Postulate H is satisfied vacuously.

(H) A class of five elements, 0, 1, 2, 3, 4 with $\oplus$ defined as in the accompanying table.

$\oplus$	0	2	3	4	1
0	0	2	3	4	1
2	2	2	1	4	1
3	3	1	3	1	1
4	4	4	1	4	1
1	1	1	1	1	1

Here A and B clearly hold. Postulate C holds, when a or b or c is 0 or 1; when $a = c$; and in the other cases by trial. Postulate G holds: $\bar{0} = 1$, $\bar{2} = 3$, $\bar{3} = 2$ or 4, $\bar{4} = 3$, $\bar{1} = 0$; but notice that $\bar{a}$ is not uniquely determined by a in the case $a = 3$. Postulate H fails in the case $a = 4$, $b = 3$, $\bar{b} = 2$. (Compare proof of independence of postulate 9 in § 2, and the unsolved problem proposed at the end of that section.)

(J) A class composed of a single element a, with $a \oplus a = a$.

Appendix.

Any system $(K, \oplus, \odot, \bar{\ })$ which obeys the laws of the algebra of logic may be called a *logical field* (a term which I venture to suggest as analogous to

"Galois field"). In this appendix * we consider all possible *finite* logical fields, that is, all possible finite classes, K, in which the rules of combination, $\oplus$ and $\odot$, and the dyadic relation, $\subset$, can be so defined as to satisfy the postulates of § 1, § 2, or § 3.

1. *The number of elements in every finite logical field must be* 2^m, where $m = 1, 2, 3, \cdots$.

For, if $a \subset b$, and $a \neq b$, we can always find an element $x \neq /\!\backslash$, namely $x = \bar{a}b$, such that $a \oplus x = b$ and $ax = /\!\backslash$. Hence, in any finite logical field we can find a set of m elements different from $/\!\backslash$, say $u_1, u_2, \cdots, u_m$, such that

$$u_1 + u_2 + u_3 + \cdots + u_m = \backslash/$$

while

$$u_i u_j = /\!\backslash \qquad (i \neq j).$$

These m elements may be called *irreducible*.

Every element except $/\!\backslash$ is then the sum of k of these irreducible elements ($1 \leqq k \leqq m$), whence, by a familiar theorem in combinations,† the total number of elements is 2^m.

2. *Any class the number of whose elements is a power of* 2, *say* 2^m, *can be made into a logical field by properly defining* $\oplus$, $\odot$ *and* $\subset$; *and this in essentially only one way.*

The process of constructing the requisite "addition-," "multiplication-," and "relation-tables" is the following:

Select one element to serve as $/\!\backslash$. Select m other elements to serve as the "irreducible" elements of the system, and denote them by $u_1, u_2, u_3, \cdots, u_m$. Select ${}_mC_2$ other elements to serve as the elements which are the sums of *two* of the irreducible elements, and denote them by u_{12}, u_{13}, u_{23}, etc., so that we shall have $u_{12} = u_1 \oplus u_2$, etc. Select ${}_mC_3$ other elements to serve as the elements which are the sums of *three* of the irreducible elements, and denote them by $u_{123}, u_{124}, u_{234}$, etc.; so that we shall have $u_{123} = u_1 \oplus u_2 \oplus u_3$, etc. And so on. Finally, $u_{123\ldots m} = \backslash/$.

The construction of the tables is then obvious. Thus, $u_A \subset u_B$ when and only when the digits in the subscript A are all contained among the digits in the subscript B; $u_A \oplus u_B = u_S$ where the subscript S contains all the digits that occur in A and also all that occur in B; $u_A \odot u_B = u_P$, where the subscript P contains only those digits which are common to the subscripts A and B.

HARVARD UNIVERSITY,
CAMBRIDGE, MASS.

* Cf. P. PORETSKII, *Théorie des égalités logiques à trois termes a, b et c;* Bibliothèque du congrès international de philosophie, Paris 1900, vol. 3 (1901), pp. 201–233; and SCHRÖDER, loc. cit., vol. 1, p. 658. The notation and method of proof here used were suggested to me by Professor E. H. MOORE.

† This theorem: $1 + {}_mC_1 + {}_mC_2 + {}_mC_3 + \cdots + {}_mC_m = 2^m$, is, oddly enough, not explicitly mentioned in CHRYSTAL's *Algebra;* see vol. 2 (2d edition), chap. XXIII, § 13.

ON THE ORDER OF LINEAR HOMOGENEOUS GROUPS*

(SECOND PAPER)

BY

H. F. BLICHFELDT

Introduction.

§ 1. In 1878 JORDAN proved a theorem concerning linear homogeneous groups which may be enunciated as follows: Every such group G in n variables has an abelian self-conjugate subgroup F of order f, and the order of G is λf, where λ is inferior to a fixed number which depends only upon n.† The proof of this theorem is quite remarkable, the more so since the limit of λ is not determined. The writer of the present article is not aware of any attempts that have been made since 1878 to find a limit to λ—aside from the cases $n = 2, 3, 4$—and he presents herewith some theorems which, in connection with some given by him in these Transactions, vol. 4 (1903), pp. 387–397, can be utilized to determine a number that λ must divide, at least in the case of "primitive" groups. However, the chief object of the present paper is not this, but rather the presentation of some methods and theorems that are useful in the construction of the groups considered. As an illustration, the primitive groups in three variables are enumerated at the end of the paper.

The technical terms and phrases defined in the paper *On the order of linear homogeneous groups*, these Transactions, vol. 4, already referred to, will be retained here. As the present article is considered a continuation of this earlier paper—to which we shall hereafter refer by *Linear groups* I—we shall begin with Theorem 8, meaning by the Theorems 1–7 those of *Linear groups* I. Unless otherwise stated, the substitutions used are linear and homogeneous in the variables concerned, and of determinant 1.

Primitive groups containing intransitive self-conjugate subgroups.

§ 2. Let H be an intransitive self-conjugate subgroup of a primitive group G in n variables. Its different systems of intransitivity may not contain the same number of variables, especially as H may possibly be exhibited as an

* Presented to the Society at the San Francisco meeting, December 25, 1903. Received for publication December 18, 1903.

† Journal für Mathematik, vol. 84 (1878), p. 89.

intransitive group in more than one way. Supposing the least number of variables that may occur in a system is a, let $x_1, x_2, \cdots, x_a$ be the variables of such a system or set, as we shall call it. Then must H be transitive in $x_1, x_2, \cdots, x_a$.

The substitutions of G cannot all leave the set $(x_1, \cdots, x_a)$ invariant (we shall say that a substitution or a group leaves a set of variables invariant if the given substitution or the substitutions of the given group transform each of the variables of the set into linear functions of the set), or G would be intransitive.* Hence, some one substitution of G must transform the set $(x_1, \cdots, x_a)$ into a new set $(y_1, \cdots, y_a)$, the variables of which are not all linear functions of $x_1, \cdots, x_a$ alone, which set must also be left invariant by H. If $y_1, \cdots, y_a$, which are evidently linearly independent of each other, were connected with $x_1, \cdots, x_a$ by b linear relations $(b < a)$, say $x_1 = y_1, x_2 = y_2, \cdots, x_b = y_b$, to which form such relations could always be brought by a proper transformation, then it is evident that H should leave invariant the set $(x_1, \cdots, x_b)$, i. e., H could not be transitive in the variables $x_1, \cdots, x_b, x_{b+1}, \cdots, x_a$.* Thus, the $2a$ variables $x_1, \cdots, x_a; y_1, \cdots, y_a$ are linearly independent.

If $2a < n$, G cannot leave the variables $(x_1, \cdots, x_a, y_1, \cdots, y_a)$ invariant. Hence, some one substitution of G must transform $(x_1, \cdots, x_a)$ into a new set $(z_1, \cdots, z_a)$, which must also be left invariant by H. If $3a < n$, we proceed in the same manner, and we get, finally, k sets of variables $(n = ka)$, linearly independent of each other,

$$(1) \qquad (x_1, \cdots, x_a), \quad (y_1, \cdots, y_a), \quad (z_1, \cdots, z_a), \quad \cdots,$$

forming the different systems of intransitivity of H.

§ 3. Now, G cannot merely permute among themselves the sets (1), or it would be imprimitive. Some one substitution of G must therefore transform the set $(x_1, \cdots, x_a)$ into a set containing variables from two or more of the sets (1), say from the second and third. Let the set obtained be

$$(2) \qquad \sum_{i=1}^{a} (\alpha_{ij} y_i + \beta_{ij} z_i) \qquad (j = 1, 2, \cdots, a),$$

which is also left invariant by H.

The expressions

$$\sum_{i=1}^{a} \alpha_{ij} y_i \qquad (j = 1, 2, \cdots, a)$$

must be linearly independent of each other, or H would be intransitive in the variables $y_1, \cdots, y_a$, by MASCHKE's theorem. Similarly, the expressions

$$\sum_{i=1}^{a} \beta_{ij} z_i \qquad (j = 1, 2, \cdots, a)$$

* MASCHKE, *Beweis des Satzes, dass diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehende verschwindende Coefficienten auftreten, intransitiv sind*, Mathematische Annalen, vol. 52 (1899), pp. 363–368.

must be linearly independent of each other. We may therefore, by a transformation affecting only the letters $y_1, \cdots, y_a$, write the set (2) in the form

$$y_1 + z_1,\ y_2 + z_2,\ \cdots,\ y_a + z_a.$$

It is readily seen that H will leave the invariant set

$$s_1 y_1 + s_2 z_1,\ s_1 y_2 + s_2 z_2,\ \cdots,\ s_1 y_a + s_2 z_a, \tag{3}$$

s_1 and s_2 being arbitrary constants.

Noticing that H could not leave invariant the set (3), and also a set of the form

$$s_1 y_i + s_2 z_i' \qquad (i = 1, 2, \cdots, a),$$

$z_1', z_2', \cdots$ being linear functions of the variables $z_1, z_2, \cdots, z_a$, unless $z_1' = \rho z_1$, $z_2' = \rho z_2, \cdots$, we can carry out the process just started, proving finally that H must leave invariant a set of the form

$$s_1 x_i + s_2 y_i + s_3 z_i + \cdots + s_k w_i \qquad (i = 1, 2, \cdots, a), \tag{4}$$

containing all the ka variables of G.

§ 4. Any substitution S of G will therefore transform the expression

$$\sum_{i=1}^{a} t_i (s_1 x_i + s_2 y_i + s_3 z_i + \cdots + s_k w_i),$$

$t_1, t_2, \cdots, t_a, s_1, s_2, \cdots, s_k$ being arbitrary constants, into the expression

$$\sum_{i=1}^{a} t_i' (s_1' x_i + s_2' y_i + s_3' z_i + \cdots + s_k' w_i),$$

where the different constants $t_1' s_1', t_2' s_1', \cdots, t_1' s_2', \cdots$, are obtained from the constants $t_1 s_1, t_2 s_1, \cdots, t_1 s_2, \cdots$, by a linear transformation, the matrix of which is the matrix transposed of the substitution S in the variables $x_1, x_2, \cdots, y_1, \cdots$. It can now be proved without difficulty that we may so choose $s_1', s_2', \cdots, t_1', t_2', \cdots$, that the letters $s_1, s_2, \cdots, s_k$ are transformed into $s_1', s_2', \cdots, s_k'$ by a linear substitution S' of determinant $\Delta' = 1$, the aggregate of which substitutions form a group G' isomorphic with G. Moreover, the letters $t_1, t_2, \cdots, t_a$ are transformed into $t_1', t_2', \cdots, t_a'$ by a linear substitution S'' of determinant Δ'', the aggregate of which form a group G'' isomorphic with G. If the matrices of S' and S'' are respectively

$$S': \begin{array}{c|cccc} & s_1 & s_2 & \cdots & s_k \\ \hline s_1 & \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ s_2 & \beta_1 & \beta_2 & \cdots & \beta_k \\ \vdots & \cdot & \cdot & \cdots & \cdot \\ s_k & \kappa_1 & \kappa_2 & \cdots & \kappa_k \end{array}, \qquad S'': \begin{array}{c|cccc} & t_1 & t_2 & \cdots & t_a \\ \hline t_1 & \lambda_1 & \lambda_2 & \cdots & \lambda_a \\ t_2 & \mu_1 & \mu_2 & \cdots & \mu_a \\ \vdots & \cdot & \cdot & \cdots & \cdot \\ t_a & \rho_1 & \rho_2 & \cdots & \rho_a \end{array},$$

that of S is

$$S: \quad \begin{array}{c|cccccc} & x_1 & x_2 & \cdots & x_a & y_1 & \cdots \\ \hline x_1 & \alpha_1\lambda_1 & \alpha_1\mu_1 & \cdots & \alpha_1\rho_1 & \beta_1\lambda_1 & \cdots \\ x_2 & \alpha_1\lambda_2 & \alpha_1\mu_2 & \cdots & \alpha_1\rho_2 & \beta_1\lambda_2 & \cdots \\ \vdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x_a & \alpha_1\lambda_a & \alpha_1\mu_a & \cdots & \alpha_1\rho_a & \beta_1\lambda_a & \cdots \\ y_1 & \alpha_2\lambda_1 & \alpha_2\mu_1 & \cdots & \alpha_2\rho_1 & \beta_2\lambda_1 & \cdots \\ \vdots & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{array}.$$

To a similarity-substitution of G will correspond similarity-substitutions of G' and G''. The determinant of S being unity by assumption, we have $(\Delta')^a(\Delta'')^k = (\Delta'')^k = 1$. It follows that the groups G' and G'' are finite.

It will be found by an inspection of S, S' and S'', that if G is primitive, G' and G'' must be primitive.

We shall say that the group G is *produced* from the two groups G' and G''. Two primitive groups G' and G'' will not necessarily produce a primitive group G. On the other hand, primitive groups in four variables will result if for G' and G'' we take any two primitive groups in two variables, combining with every substitution S' of G' every substitution S'' of G'', in the manner shown.

We shall embody our results in the following

THEOREM 8. *If G, a primitive group in n variables, has an intransitive, non-abelian, self-conjugate subgroup H, then is $n = ka$, where k is the number of systems of intransitivity of H containing the least number of variables $a > 1$. By a proper choice of variables we can arrange these in k sets*

$$x_1, x_2, \cdots, x_a; \qquad y_1, y_2, \cdots, y_a; \qquad \cdots; \qquad w_1, \cdots, w_a;$$

so that H leaves invariant the system

$$s_1x_i + s_2y_i + \cdots + s_kw_i \qquad (i = 1, 2, \cdots, a),$$

$s_1, s_2, \cdots, s_k$ being arbitrary constants

Groups whose orders are powers of primes.

§ 5. DEFINITION. If the variables $x_1, x_2, \cdots, x_n$ of a group G may be so selected that the substitutions of G are all of the form

$$x_i' = \alpha_i x_{\lambda_i} \quad (i = 1, 2, \cdots, n;\ \lambda_1, \lambda_2, \cdots, \lambda_n = 1, 2, \cdots, n;\ \lambda_i \neq \lambda_j),$$

then we shall say that the group may be written in *semi-canonical* form.

THEOREM 9. *A group whose order is a power of a prime can be written in semi-canonical form.*

We begin by proving that a group of degree $n > 1$ and of order p^a, p being a prime, is always intransitive or imprimitive.

For a group G of order p^a is either abelian or it must contain an abelian self-conjugate subgroup whose substitutions are not all similarity-substitutions. In both cases the theorem would be true (Theorem 2).

To show the existence of such a subgroup, if G is non-abelian, we may proceed as follows. We can form a series of groups G, G_1, G_2, $\cdots$ of orders p^a, p^{a-1}, p^{a-2}, $\cdots$, each of which is a self-conjugate subgroup of those that precede it.* The substitutions of G_1 cannot all be self-conjugate substitutions of G, the number of which is at most p^{a-2}.† Therefore if G_1 is abelian, the proposition is proved. If G_1 is non-abelian, consider G_2. Its substitutions cannot all be self-conjugate substitutions of G_1, etc. We finally arrive at an abelian self-conjugate subgroup of G of the required character.

We shall now prove Theorem 9 for a transitive group in n variables, assuming it true for any group of order p^m in less than n variables. Under this assumption the theorem follows for an intransitive group in n variables.

For a transitive and imprimitive group G of order p^a the variables must fall into p^b sets ($n = kp^b$) which are permuted according to a substitution-group in p^b letters. These may easily be shown to fall into p systems of imprimitivity. Hence, the variables of G may be separated into p sets of n/p variables each, and G is generated by an intransitive group G', which leaves each of these sets invariant, and a substitution T which permutes them according to a circular substitution of order p. We shall merely illustrate the remainder of the proof by the special case $p = 3$, $n = 6$. We may exhibit G' in the form

$$G' = \begin{vmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{vmatrix},$$

G_1 being a group in two variables, x_1, x_2 of order 3^c, and can therefore, by assumption, be written in semi-canonical form. Without transforming the variables x_1 and x_2, we may write T in the form

$$x_1' = x_3, \qquad x_2' = x_4, \qquad x_3' = x_5, \qquad x_4' = x_6,$$
$$x_5' = \alpha x_1 + \beta x_2, \qquad x_6' = \gamma x_1 + \delta x_2.$$

As T^3 belongs to G', the matrix $\left|\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right|$ must be found among those of G_1, so that $\alpha\beta = \gamma\delta = 0$. Noting that, if S_1 and S_2 are written in semi-canonical forms, so is $S_3 = S_1 S_2$, we readily see the truth of Theorem 9.

On the orders of the substitutions of a primitive group.

§ 6. DEFINITIONS. Let E be the sum of a finite number of roots of unity. Each of these can be written as the product of one (θ) whose index is a power

* BURNSIDE, *Theory of Groups*, p. 64.

† Ibid., p. 63.

of p (a prime), and one of index m, a number prime to p. Then, if every root θ be replaced by 1, the resulting value of E shall be denoted by $(E)_p$. It follows from KRONECKER's Theorem (see § 3, *Linear groups* I) that if $E=0$, then is $(E)_p = pF$, where F is the sum of a finite number of roots of unity. We shall write this equation in the form

$$(E)_p \equiv 0 \pmod{p}.$$

The multipliers of a substitution are roots of unity. The *number* of these roots that are different from one another shall be called the *variety* of the substitution. Thus, a similarity-substitution is of variety 1.

THEOREM 10. *If a group G in n variables has a substitution S of variety m and of order $p^{a+c} \geqq mp^c$, then will G contain a self-conjugate sub-group H containing $S^{p^a} = T$ and all further substitutions of G which possess the property*

$$(V)_p \equiv (VT)_p^* \pmod{p}, \tag{5}$$

V being any substitution of G. In particular, $n \equiv (T)_p \pmod{p}$.

§ 7. We begin by proving that (5) holds if $T = S^{p^a}$. Supposing ϕ to be a primitive root of the equation $\phi^{p^{a+c}} - 1 = 0$, let $(S) = \phi + \phi^\alpha + \phi^\beta + \cdots$. Form the equation corresponding to the equation (3) of *Linear groups* I,

$$\begin{vmatrix} (V) & 1 & 1 & 1 & \cdots \\ (VT) & \phi^{p^a} & \phi^{\alpha p^a} & \phi^{\beta p^a} & \cdots \\ (VS) & \phi & \phi^\alpha & \phi^\beta & \cdots \\ (VS^2) & \phi^2 & \phi^{2\alpha} & \phi^{2\beta} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (VS^{m-1}) & \phi^{m-1} & \phi^{\alpha(m-1)} & \phi^{\beta(m-1)} & \cdots \end{vmatrix} = (V)A_0' - (VT)A_1' + \cdots = 0. \tag{6}$$

Each of the determinants A_i' may be divided by A_1', and in the quotients, as well as in the weights $(V), \cdots$, unity may be substituted for ϕ. There results the congruence

$$(V)_p \left(\frac{A_0'}{A_1'}\right)_p - (VT)_p + \cdots \equiv 0 \pmod{p}.$$

By the method of § 5, *Linear groups* I, we get

$$\left(\frac{A_0'}{A_1'}\right)_p \equiv 1 \pmod{p}; \quad \left(\frac{A_i'}{A_1'}\right)_p \equiv 0 \pmod{p} \qquad (i>1),$$

so that (5) follows.

* The sum of the multipliers of a substitution S was in *Linear groups I* designated by (S) and called the *weight* of S. In a paper by BURNSIDE, Proceedings, London Mathematical Society, November, 1903, pp. 117–123, it is called the *characteristic* of S, and the different characteristics contained in a group G are proved to satisfy the conditions for a set of *Gruppencharaktere* in the theory of FROBENIUS. The term *weight* shall be used in the present paper, for the sake of uniformity of terminology with the paper *Linear groups I.*

We prove next that all the substitutions of G possessing this property form a group (H). Let T_1 and T_2 be any two such, then

$$(V)_p \equiv (VT_1)_p \text{ (mod. } p), \qquad \text{and} \qquad (VT_1)_p \equiv (VT_1T_2)_p \text{ (mod. } p).$$

Hence

$$(V)_p \equiv (VT_1T_2)_p \text{ (mod. } p).$$

Finally, to prove that H is self-conjugate in G, we note that, for any two substitutions A and B, $(A) = (BAB^{-1})$. Hence, if T belongs to H, and V and W to G, we have by (5),

$$(V)_p \equiv (W^{-1}VW)_p \equiv (W^{-1}VWT)_p \equiv (VWTW^{-1})_p \text{ (mod. } p).$$

§ 8. We might remark that in order to have

$$(T^i)_p \equiv n \text{ (mod. } p) \qquad (i = 1, 2, \cdots),$$

it is necessary that the number of times in which a given root, whose index is prime to p, occurs among the multipliers of T must be a multiple of p. For, let all the roots of $(T)_p$ be expressed in terms of a single root θ of index k, prime to p, so that

$$(T)_p = a + b\theta + c\theta^2 + \cdots + m\theta^{k-1}, \qquad a + b + c + \cdots + m = n.$$

Then since $(T^i)_p \equiv n \text{ (mod. } p)$, and $\theta^l + \theta^{2l} + \theta^{3l} + \cdots + \theta^{kl} = 0$, where l is any integer not divisible by k, we have

$$\sum_{i=1}^{k} \theta^{-i}\{(T^i)_p - n\} = kb \equiv 0 \text{ (mod. } p).$$

Evidently b is a multiple of p. In the same way $c, \cdots, m$ are multiples of p.

It follows that if $p > n/2$, then is $(T)_p = n$, so that the order of T is a power of p. Hence, if G contains a substitution T of order $p^{a+c} \geqq np^c$, where $p > n/2$, then will G contain a self-conjugate subgroup H whose order is a power of p. This subgroup will contain the substitution T^{p^a}. If $p > n$, H is abelian (Theorem 3), and by referring to Theorem 2 we deduce the

COROLLARY 1. *A primitive group in n variables cannot contain a substitution of order p^2, if p is a prime $> n$.*

If $p = n$, H may be imprimitive. In any event, the group H' generated by the pth powers of the substitutions of H is abelian, but may, in this case, reduce to the group of similarity-substitutions of order n. We have therefore the

COROLLARY 2. *If a primitive group G in n variables (n being a prime) contains a substitution T of order n^a, then will G contain an imprimitive or abelian self-conjugate subgroup of order n^k, containing the substitution T^n. The substitution T^{n^2} must be a similarity-substitution or identity. In any event, $a < 4$.*

If $n/2 < p < n$, H must be intransitive, and at least one of its systems of intransitivity contains only one variable (Theorem 9). A primitive group could, therefore, not contain such a group self-conjugately (Theorem 8). We readily derive the

COROLLARY 3. *A primitive group in n variables cannot contain a substitution of order p^3, p being a prime, and $n/2 < p < n$.*

§ 9. THEOREM 11. *Let G contain two permutable substitutions S and T, which can therefore be written simultaneously in canonical form. Let it be given that to equal multipliers of S correspond equal multipliers of T, so that the variety of T is not greater than that of S. Furthermore, let it be given that the order (k) of S is greater than its variety (m), and that the order of T is a prime (p), not dividing k. Then will G contain a self-conjugate subgroup H, containing T, of the same characteristic property as the group H of the Theorem* 10.

Starting with the equation corresponding to (6), we deduce the equation

$$(V)_p(A_0')_p - (VT)_p(A_1')_p + (VS)_p(A_2')_p \cdots \equiv 0 \pmod{p}.$$

We find $(A_i')_p \equiv 0 \pmod{p}$, $i > 1$; and

$$(A_0')_p \equiv (A_1')_p \equiv (\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\cdots \equiv q \pmod{p},$$

say, $\alpha, \beta, \gamma, \cdots$ being the different multipliers of S. Hence,

$$q\{(V)_p - (VT)_p\} \equiv 0 \pmod{p}. \tag{7}$$

Let β/α be a primitive rth root of unity, r being a factor of k and therefore prime to p. Then is $\alpha - \beta$ a factor of

$$(\alpha-\beta)(\alpha^2-\beta^2)\cdots(\alpha^{r-1}-\beta^{r-1}) = r\alpha^{r(r-1)/2}.$$

The congruence (7) may therefore be changed into the congruence (5) by multiplying both sides of (7) by a certain expression which is the sum of a finite number of roots of unity.

§ 10. Let the multipliers of the substitution T be denoted by $\alpha_1, \alpha_2, \cdots, \alpha_n$, so that

$$(T) = \sum_{i=1}^{n} \alpha_i.$$

Let us form the quantities

$$(T)' = \sum \alpha_i\alpha_j, \ (T)'' = \sum \alpha_i\alpha_j\alpha_k, \cdots \quad (i, j, k, \cdots = 1, 2, \cdots, n;\ i \neq j \neq k \neq \cdots).$$

Let the number of roots in (T) that are different from one another be m_1 (the variety of T), the number of the $\frac{1}{2}n(n-1)$ products of $(T)'$ that are distinct be m_2, etc. Then we shall, for the present, call the greatest of the numbers

$m_1, m_2, \cdots$ the *rank* of T, and denote it by M. Evidently $M \leqq {}_nC_{n/2}$ if n is even, and $M \leqq {}_nC_{(n+1)/2}$ if n is odd.

THEOREM 12. *If a group G of degree n contains a substitution T of rank M and of order $p^{a+c} \geqq Mp^c$, p being a prime, then will G contain a self-conjugate sub-group of order p^k which will contain a substitution of order p^c, namely T^{p^a}.*

Let S be T^{p^a}. We shall first prove that if V be any substitution of G, then will the order of VS contain no other prime factors than p and those contained in the order of V. Let the variables of G be so chosen that T is written in canonical form. By theorem 10 we have

$$(V)_p \equiv (VS)_p \pmod{p}.$$

Moreover, the method employed to prove this theorem may be used in exactly the same manner to prove that we have

$$(8) \qquad \begin{cases} (V)' \equiv (VS)'_p \pmod{p}, \\ (V)'' \equiv (VS)''_p \pmod{p}, \\ \cdots\cdots\cdots\cdots \end{cases}$$

As the two sets of quantities $(V), (V)', \cdots; (VS), (VS)', \cdots$ are, respectively, the elementary symmetric functions of the multipliers of V and VS, which multipliers shall be designated by $\epsilon_1, \epsilon_2, \cdots, \epsilon_n; \zeta_1, \zeta_2, \cdots, \zeta_n$, we must have

$$\{(\rho-\epsilon_1)(\rho-\epsilon_2)\cdots(\rho-\epsilon_n)\}_p \equiv \{(\rho-\zeta_1)(\rho-\zeta_2)\cdots(\rho-\zeta_n)\}_p \pmod{p},$$

for every value of ρ. Hence

$$\{(\zeta_i-\epsilon_1)(\zeta_i-\epsilon_2)\cdots(\zeta_i-\epsilon_n)\}_p \equiv 0 \pmod{p},$$

and therefore also

$$(9) \qquad \{(\zeta_i^k-\epsilon_1^k)(\zeta_i^k-\epsilon_2^k)\cdots(\zeta_i^k-\epsilon_n^k)\}_p \equiv 0 \pmod{p}.$$

Suppose it possible that the order of VS contain a prime factor $q \neq p$ and not contained in the order of V. Then we may choose k such that the congruence (9) becomes

$$(\eta-1)^n \equiv 0 \pmod{p},$$

the index of η being q. But this congruence is an impossibility, $\eta - 1$ being a factor of q.

Now, as in the case of the Theorem 10, all the substitutions possessing the properties of the substitution S, indicated by the congruences (8), form a group H, self-conjugate in G. All the substitutions of this group whose orders are powers of p must, by what has just been proved, form a group whose order is a power of p, and this group is plainly contained in G self-gonjugately. But

among the substitutions of this group is T^{α} (called S in the proof), a substitution of order p^{c}. Hence the theorem.

§ 11. THEOREM 13. *If the group G contains two substitutions S and T, of orders p and q (different prime numbers > 2) respectively, whose weights do not contain all the primitive pth and qth roots of unity, then will G contain a substitution of order pq.*

Consider the system of equations (2) of *Linear groups* I, under the condition $v = 1$. Assuming that the list $\alpha, \beta, \cdots, \kappa$ does not include all the roots of $(\theta^{p} - 1)/(\theta - 1) = 0$, let ρ be one such different from $\alpha, \beta, \cdots, \kappa$. Then is evidently

$$(T) + \rho^{-1}(ST) + \rho^{-2}(S^{2}T) + \cdots + \rho^{-p+1}(S^{p-1}T) = 0.$$

The assumption that none of the weights (ST), $(S^{2}T)$, $\cdots$ contain both pth and qth roots of unity is untenable, which can be seen as follows. Under the assumption, suppose at least one of these weights, $(S^{i}T)$, contains pth roots. We will transpose all the corresponding terms $\rho^{-i}(S^{i}T)$, and by means of the relation $1 + \rho + \rho^{2} + \cdots + \rho^{p-1} = 0$ we can change the right-hand member of the resulting equation into such a form that this becomes an identity in ρ. Then (T) = sum of roots of unity, the indices of which are prime to q. But this is impossible, since (T) contains only qth roots and is not equal to an integer, as at least one qth root is absent by assumption. Thus, none of the weights of the equation considered can contain pth roots. In this event the equation can be true only if $(T) = (ST) = \cdots = (S^{p-1}T)$. Similarly we find $(S) = (ST) = \cdots = (ST^{q-1})$. Hence $(T) = (S)$, an impossibility. Accordingly, at least one of the weights considered must contain both pth and qth roots of unity, and the theorem is proved.

COROLLARY. *A group G of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} N$, where $p_1, p_2, \cdots, p_m$ are primes each greater than $n + 1$, contains an abelian subgroup of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.*

To prove this corollary, we may assume it true for all groups in less than n variables. It follows immediately for all intransitive groups in n variables. Let us therefore consider a transitive group G of the order given. A substitution S of order $p > n + 1$ will fulfill the condition of the Theorem 13. Hence, the group G contains a substitution of order $p_1 p_2$, which can evidently be written as the product of two substitutions A and B, of orders p_1 and p_2 respectively. The subgroup of G of order p_1^{α} to which A belongs being abelian, this group and the substitution B will generate an intransitive group, containing the substitution A self-conjugately. The order of this group is divisible by $p_1^{\alpha} p_2$. For such a group the corollary has been proved true. There results that we have an abelian subgroup of G of order $p_1^{\alpha} p_2$, the product of a group G_1 of order $p_1^{\alpha_1}$ and a substitution C of order p_2. But this substitution is

contained in an abelian subgroup G_2 of G of order $p_2^{\alpha_2}$. The groups G_1 and G_2 will therefore generate an intransitive group, whose order is divisible by $p_1^{\alpha_1} p_2^{\alpha_2}$. This has an abelian subgroup H_2 of order $p_1^{\alpha_1} p_2^{\alpha_2}$. In the same way we find that G contains an abelian subgroup H_3 of order $p_1^{\alpha_1} p_3^{\alpha_3}$. We may, obviously, assume that H_2 and H_3 have in common a group of order $p_1^{\alpha_1}$. Then will H_2 and H_3 generate an intransitive group, etc.

§ 12. We have now the means in hand whereby to determine a limit to the order of the primitive groups in n variables. It was shown in *Linear groups* I how we can obtain the limit to the highest prime which may divide the order g of such a group G. We shall now proceed to find a superior limit to the power of a prime p contained in the order of the group. We shall by p^{n_p} denote the highest power of p which divides $n!$.

Let p^N be the highest power of p which divides g. Then G contains a subgroup of order p^N, and this again an abelian subgroup G' of order $g' \geqq p^{N-n_p}$, if $N > n_p$ (Theorem 9). Let G' be written in canonical form. Then it is plain that we can have no more than $p^{n-1} - 1$ substitutions of order p contained in G'; no more than $p^{2(n-1)} - 1$ substitutions of orders p^2 and p, and so on. Therefore, if $p^a \geqq n > p^{a-1}$, and $N - np > (n-1)(a+c-1)$, G will contain a self-conjugate subgroup H containing a substitution of order p^c, this subgroup being of the kind considered in the Theorem 10. Again, if

$$p^a \geqq \frac{n!}{(n/2!)^2} > p^{a-1} \qquad \text{when } n \text{ is even,}$$

or

$$p^a \geqq \frac{n!}{(n-1)/2!\,(n+1)/2!} > p^{a-1} \quad \text{“} \quad \text{“} \quad \text{“ odd,}$$

and if

$$N - n_p > (a+c-1)(n-1),$$

then will G, according to the Theorem 12, contain a self-conjugate subgroup K of order p^k, containing a substitution of order p^c.

Suppose $n = n_1 p^a$, where $n_1 = 1$ or is prime to p. Then will the p^ath powers of the substitutions of K generate an intransitive group L which will contain a substitution of order $p^{c-\alpha}$, if $c > \alpha$. Now, at least one of the systems of intransitivity of L contains only one variable. Accordingly, since L is a self-conjugate subgroup of G, this could not be primitive unless the substitutions of L are all similarity-substitutions (Theorem 8). This could not be the case, however, if $c - \alpha > \alpha$.

Therefore, if G is primitive, and its order is divisible by p^N, then must

$$N \leqq n_p + (a + 2\alpha)(n-1).$$

But,

$$n_p < \frac{n}{p-1}, \qquad \alpha \leqq \frac{\log n}{\log p}, \qquad \text{and} \qquad a < 1 + \frac{\log A}{\log p},$$

A being the highest term in the expansion of $(1+1)^n$. Hence,

$$N < \frac{n}{p-1} + \left(1 + \frac{\log n^2 A}{\log p}\right)(n-1).$$

This number is evidently a great deal higher than necessary. In any given case it may be reduced by a closer inspection of the subgroups of order p^N. We have assumed that the substitutions considered are of variety n, whereas this may be much less in special cases. Theorems 10, 11 and 13 and their corollaries may be used to advantage, especially in the case of simple groups.

In any event, a number can now be found which the order of a primitive group of substitutions of determinant 1 must divide. If the determinants of the substitutions of a group G are not all $= 1$, we may write each of these in the form SA, where A is a substitution of determinant 1 and S a similarity-substitution. The substitutions A will form a group G' whose order λ is a factor of the order of G, and we can tabulate the substitutions of G in such a manner as to show that the order of G is λf, where f is the order of a group F of similarity-substitutions, contained self-conjugately in G. If G is primitive, so is G', and we have, accordingly, proved JORDAN's Theorem (Introduction) for primitive groups and are, moreover, able to give in any special case a number that λ must divide.

The primitive groups in three variables.

§ 13. We shall consider in order the three cases:

A. Primitive groups having imprimitive self-conjugate subgroups.

B. Primitive groups which are simple.

C. Primitive groups which have intransitive self-conjugate subgroups.

D. Primitive groups having primitive self-conjugate subgroups.

A. Let G be a primitive group having an imprimitive self-conjugate subgroup H. By studying the different possible cases of imprimitive groups, which are all of the type

$$x_1' = \alpha x_i, \qquad x_2' = \beta x_j, \qquad x_3' = \gamma x_k \qquad (i, j, k = 1, 2, 3;\ i \neq j \neq k),$$

and by taking for H the group generated by the 2nd powers of the substitutions of such a group, we find readily that either the 3rd powers of the substitutions of H will generate an abelian group which is not merely the group of similarity-substitutions, or H will contain substitutions of order 3, and possibly of order 9 and variety 2. In the first case, G could not be primitive, since the abelian group obtained from H in the manner indicated is contained self-conjugately in G. In the second case, H will contain self-conjugately the group H' generated by the substitutions

$$P: \quad x_1' = x_2,\ x_2' = x_3,\ x_3' = x_1;$$

$$Q: \quad x_1' = x_1,\ x_2' = \omega x_2,\ x_3' = \omega^2 x_3 \qquad (\omega^3 = 1,\ \omega \neq 1);$$

and is itself generated by this group and the substitution

$$R: \quad x_1' = \phi x_1,\ x_2' = \phi x_2,\ x_3' = \phi\omega^2 x_3 \qquad (\phi^3 = \omega),$$

if it does not coincide with H'.

The group H possesses the relative invariant $x_1x_2x_3$, and this is the only one of the third order if the substitution R be present in H, whereas the group H' possesses a set of four that can each be resolved into linear factors, namely

$$(10) \qquad x_1x_2x_3;\ x_1^3 + x_2^3 + x_3^3 - 3\theta x_1x_2x_3 \qquad (\theta = 1, \omega, \omega^2).$$

If H contains R, G is evidently imprimitive, as it should then leave invariant, to a constant factor, the function $x_1x_2x_3$. Hence, G must contain H' self-conjugately, and must permute among themselves the invariants (10). Imposing upon the substitutions of G this condition, it is easily found that the generating substitutions of G, aside from P and Q, are

$$S: \quad \rho x_1' = x_1 + x_2 + x_3,\ \rho x_2' = x_1 + \omega x_2 + \omega^2 x_3,\ \rho x_3' = x_1 + \omega^2 x_2 + \omega x_3,$$
$$\rho = \omega - \omega^2;$$

$$T: \quad \rho x_1' = x_1 + \omega x_2 + \omega x_3,\ \rho x_2' = \omega^2 x_1 + \omega x_2 + \omega^2 x_3,$$
$$\rho x_3' = \omega^2 x_1 + \omega^2 x_2 + \omega x_3,\ \rho = \omega - \omega^2$$

$$U: \quad \phi\rho x_1' = \omega^2 x_1 + \omega^2 x_2 + \omega^2 x_3,\ \phi\rho x_2' = \omega x_1 + \omega^2 x_2 + x_3,$$
$$\phi\rho x_3' = \omega x_1 + x_2 + \omega^2 x_3,\ \rho = \omega - \omega^2;$$

where $\phi^3 = \omega$.

The substitutions S, S and T, S and U, and the group H' generate, respectively, primitive groups of orders 108, 216 and 648. They all contain the group F of similarity-substitutions (contained in H'), and their quotient-groups (abstract groups) $G' = G/F$, of orders 36, 72 and 216, are the *Hessian group* and some of its subgroups, discussed by Jordan in his determination of the linear groups in three variables.*

§ 14. *B.* By Theorem 5, the order of a primitive group G in 3 variables is of the form $2^a3^b5^c7^d$. By Theorem 10, Corollaries 1–3, we can have no substitutions of orders 8, 81, 25 or 49. If there is a substitution of order 27, G contains a self-conjugate subgroup H of order 3^k containing a substitution of order 9, which is not a similarity-substitution. The group H is abelian or imprimitive, and G would be imprimitive or intransitive in either case (cf. case *A*). In the same way we find that G cannot contain a substitution of order 9, the 3d power of which is not a similarity-substitution.

We now find, by studying the groups of orders 2^a, 3^b, 5^c, 7^d in detail, that

1°. $a \leqq 3$; 2°. $b \leqq 4$; 3°. c (and d) $\leqq 2$;

4°. If $b \geqq 3$, there is a similarity-substitution;

* Journal für Mathematik, vol. 84 (1878), p. 89.

5°. If $b = 4$, there is a substitution of order 9 and variety 2;

6°. If c (or d) $= 2$, there is a substitution of order 5 (or 7) and of variety 2. We shall prove that we can have no substitution of order 5 and of variety 2. Let, if possible, S be such a substitution. Its weight may be written $a + a + a^3$, where $a^5 = 1$. Then, if A be any substitution of G, we have

$$(A)\frac{\alpha^{3r+1} - \alpha^{r+3}}{\alpha^3 - \alpha} - (AS)\frac{\alpha^{3r} - \alpha^r}{\alpha^3 - \alpha} + (AS^r) = 0,$$

an equation obtained in the same manner as equation (6). Hence,

$$(11) \qquad (A)_5(r-1) - (AS)_5 r + (AS^r)_5 \equiv 0 \pmod 5.$$

Let A be of order 5. Then $(A)_5 = 3$. It is plain that $(AS)_5$ cannot contain 7th roots of unity. In fact, we find without much trouble that the order of AS must be a factor of 30. The weight of this substitution is therefore of the form $\epsilon_1 + \epsilon_2 + \epsilon_3 = 1$, where $\epsilon_1^{30} = \epsilon_2^{30} = \epsilon_3^{30} = 1$. It follows that $(AS)_5$ must have one or other of the values

$$(12) \qquad 0, -1, \pm 2, -\omega, -\omega^2, \pm 2\omega, \pm 2\omega^2, \pmod 5.$$

Moreover, the value of $(AS^r)_5$ is found in the same way to be one of the quantities (12). Substituting, therefore, the different quantities (12) in (11), taking different values for r, we find that the only value possible for $(AS)_5$ is -2 (mod. 5), i. e., the substitution AS must be of order 5 or 1.

From this it follows that all the substitutions of G of order 5 form a group, in which case G could not be primitive (Theorems 2, 3). For, from what has just been proved, the product of any substitution of order 5 and one of order 5 and variety 2 is a substitution of order 5. Now, if we have *one* substitution of order 5 and variety 2, any substitution of order 5 can be written as the product of two substitutions, each of order 5 and variety 2, which we see when we write any subgroup of G of order 5^k in canonical form, bearing in mind that conjugate substitutions have the same multipliers.

In the same way we can prove that G cannot contain a substitution of order 7 and variety 2. It follows that the order of G is not divisible by 25 or by 49. Nor is it divisible by 5.7, for we have in such a case a substitution of order 5.7 (Theorem 13), which we could write as the product of two of orders 5 and 7 respectively, permutable with each other. Since neither of these could be of variety 2, we could employ Theorem 11 to prove that G would contain a self-conjugate subgroup of order 7; an impossibility.

If the order of G is divisible by 5 or by 7, G cannot contain a substitution of order 9 and variety 2. For, let S be of order 5, and T of order 9 and variety 2, and let $(T) = \phi + \phi + \phi\omega^2$, where $\phi^3 = \omega$, $\omega^3 = 1$, $\omega \neq 1$. The equation corresponding to (6) is here

$$(S) + \omega\phi^2(ST) + \phi(ST^2) = 0.$$

We see at once that either (ST) or (ST^2) must contain both 5th and 9th roots of 1. There would result a substitution of order 5.9. The group G would contain a self-conjugate subgroup of order 3^k (Theorem 11), containing a substitution of order 9, and could not be primitive (Cf. case A). Similarly, G cannot contain a substitution of order 7 and one of order 9 and variety 2.

Referring now to the list of conditions 1°–6°, we find that the order of G is a factor of one of the following numbers.

I. G does not contain similarity-substitutions:

$$2^3 3^3, \quad 2^3 3^2 5, \quad 2^3 3^2 7;$$

II. G contains the group of similarity-substitutions:

$$2^3 3^4, \quad 2^3 3^3 5, \quad 2^3 3^3 7.$$

§ 15. The orders of the simple groups desired are factors of the numbers of the series I, the greatest of which is 504. As is well known, there are only four types of abstract simple groups whose orders are less than 505, namely, groups of orders 60, 168, 360 and 504. This last group contains an abelian subgroup of order 8, all of whose substitutions are of order 2.* Such an abelian group cannot, however, be constructed as a linear group in 3 variables, which is apparent when we attempt to write it in canonical form. The abstract simple group of order 360 contains a subgroup of order 9. When we attempt to construct linear homogeneous groups in 3 variables of order 9, we find that they will contain either a similarity-substitution or a substitution of order 9 and of variety 2. The latter substitution is excluded from a primitive group containing a substitution of order 5, and the former could not be contained in a simple group. Thus, only the cases of orders 60 and 168 could furnish us primitive groups in 3 variables. That two such groups, one type of each, do exist is well known.†

§ 16. *C.* We come now to primitive groups having self-conjugate intransitive subgroups. By theorem 8 it appears that no primitive group G in 3 variables can have such a subgroup unless this is the group F of similarity-substitutions. The quotient-group (existing as an abstract group) $G' = G/F$ must be simple, or G would contain a self-conjugate subgroup different from the group F. The order of G being a factor of one of the numbers of the series II., that of G' must be a factor of one of the numbers of the series I. We obtain, for the order of G', one of the numbers 60, 168, 360 or 504.

As shown above, the case 504 may be dismissed. The case 360 can not be thrown out by the reasons given in § 15. In fact, a group of order 360 iso-

*BURNSIDE, *Theory of Groups*, p. 373; COLE, American Journal of Mathematics, vol. 15 (1893), pp. 303–315.

†See WIMAN, Mathematische Annalen, vol. 47 (1896), pp. 532–533, and Encyclopädie der Mathematischen Wissenschaften, Bd. 1, Heft 5 (1900), pp. 528–530, for references. See also MASCHKE, Mathematische Annalen, vol. 51 (1899), pp. 259–269.

morphic with the abstract simple group of order 360 and containing the group of similarity-substitutions can be represented as a linear homogeneous group in 3 variables.* Groups of orders 3.60 and 3.168, isomorphic with the abstract simple groups of orders 60 and 168 respectively, and containing the group F, can also be constructed as linear homogeneous groups in 3 variables. We need only construct the groups $\{G_{60}, F\}$, $\{G_{168}, F\}$; G_{60} and G_{168} denoting the primitive groups of orders 60 and 168 mentioned in § 15.

§ 17. *D.* We come, finally, to primitive groups having primitive self-conjugate subgroups. — With each of the primitive groups already obtained is associated a system of invariants.* An examination of these invariants and of the conditions given in § 14 will disclose the fact that any one of the primitive groups given is contained self-conjugately only in itself or in the group generated by a similarity-substitution and the group itself, excepting the case of the G_{108}, which is contained self-conjugately in the G_{216}, and this again in the G_{648}.

The primitive groups in three variables, linear and homogeneous, have now been enumerated. We have found the orders 648, 216, 108, 1080, 60, 168. (180, 504). The groups of orders 180, 504 are isomorphic with the groups of order 60 and 168 respectively.*

* Cf. WIMAN, Mathematische Annalen, vol. 47 (1896), pp. 532–533.

ALGEBRAS DEFINED BY FINITE GROUPS*

BY

JAMES BYRNIE SHAW

Introduction.

1. In a paper presented to this Society at a previous meeting, † the general structure of linear associative algebra was discussed and certain fundamental theorems of great generality were proved. The present paper is an application of these theorems to the study of what may be called *group algebras*. By a group algebra is meant that linear algebra whose units are defined to be such that each unit e_i corresponds to an operator O_i of some given abstract finite group, ‡ and conversely, and such that for each equation of the group $O_i O_j = O_k$ corresponds an equation $e_i e_j = e_k$ of the algebra. From the symbolic point of view the algebra differs from the group only in that expressions—for brevity, let us say, numbers—of the form $\Sigma x_i e_i$ are possible, wherein the coefficients x_i are any scalars. § That this algebra is linear and associative, is obvious from the definition. When no confusion is feared, the notations and terminology of the group and of the algebra will be used interchangeably.

2. In the paper cited as *Theory* is developed the theorem that the numbers of a linear associative algebra are subject to the laws of matrices, and certain conclusions are drawn from this fact. This method of development enables us to make immediate use of any theorem needed which is true of matrices, and so saves a redevelopment of many such theorems. In the present paper I shall consider the numbers as multiple algebraic entities, referring to the theory of matrices only when some needed theorem is to be translated into an algebraic theorem.

3. In Part 1 of the paper the general form of any group algebra is to be discussed and certain general theorems established. In Part 2 a few special cases

* Presented to the Society (St. Louis) Dec. 31, 1903. Received for publication January 12, 1904.

† *Theory of Linear Associative Algebra*, Transactions of the American Mathematical Society, vol. 4 (1903), pp. 251–287. This paper is hereafter cited as *Theory*.

‡ It was POINCARÉ, *Sur l'intégration algébrique des équations linéaires et les périodes des intégrales abéliennes*, Journal de Mathématiques, ser. 5, vol. 9 (1903), pp. 139–213, who first made such a correspondence (p. 183)—Cf. also A. YOUNG, Proceedings of the London Mathematical Society, vol. 33 (1900–01), p. 97, where expressions linear and homogeneous in literal substitutions are used as operators.

§ I. e., for the present purposes, ordinary complex numbers.

are considered, in order to elucidate the theory and to furnish comparisons with other well-known methods.* In Part 2, § 1, it is shown that every abelian group of order n defines the same group algebra. Professor E. H. MOORE has pointed out that this result is not equally true for all fields of coefficients. This paper relates only to the scalar continuous field. In general we have the question to study: *With respect to any field of coefficients, what groups determine the same algebra, and what common property do such groups have?* In Part 3 is considered the ultimate connection of this theory with FROBENIUS's theory of group characters and group determinants, BURNSIDE's continuous groups defined by finite groups, and DICKSON's theory of groups in an arbitrary field defined by finite groups. In anticipation as well as summary it may be said that the present theory seems to furnish a desirable common ground for all these theories.

4. The theorem that *every group algebra is semi-simple or matric* (Part 1, § 3) was proved by POINCARÉ, in the article cited,† by connecting the work of MOLIEN and CARTAN‡ on linear associative algebras from the standpoint of continuous groups, with that of FROBENIUS on the group determinants arising from groups of finite order. On the basis of the *Theory* a direct proof of this theorem is given in Part 1. The general theory of matric algebras will be developed later.

PART 1. GENERAL THFOREMS.

1. For present purposes I proceed to state certain propositions — theorems or obvious deductions from theorems of the general theory.

Since the numbers of a linear associative algebra are subject to the theorems of matrices, it follows that a number satisfies a certain irreducible equation with scalar coefficients — the characteristic equation of the number; the degree of this equation is the degree of the number. — The general number, with indeterminate scalar coefficients x_i, satisfies the characteristic equation of the algebra, a certain irreducible equation, with coefficients polynomials in the indeterminates x_i, with scalar coefficients — the characteristic equation of the algebra;

* The special examples chosen are the algebras derived from *cyclic groups* § 1, *abelian groups* § 1, *the dihedron groups* § 2, *the symmetric groups on three and four letters* §§ 2, 4, *the tetrahedral group* § 3, and *a certain group of order* 16 § 5.

† loc. cit., pp. 184–186.

‡ MOLIEN, *Ueber Systeme höheren complexen Zahlen*, Mathematische Annalen, vol. 41 (1893), p. 83; vol. 42 (1893), p. 308.

CARTAN, *Les groupes bilinéaires et les systèmes de nombres complexes*, Annales de Toulouse, vol. 12 (1898).

The results and methods of MOLIEN and of CARTAN are closely related, although neither CARTAN nor POINCARÉ refers to MOLIEN. In particular, CARTAN's simple systems or p^2-ions, the generalization of quaternions and nonions, (the quadrate algebras of this paper) are MOLIEN's primitive (ursprüngliche) systems.

the degree of this equation is the degree of the algebra; the degree of an algebra in n units is at most n or $n+1$ (according as the algebra has or has not a modulus). It may happen that the degree of every number of an algebra is less than the degree of the algebra itself, every equation resulting from the characteristic equation of the algebra by the substitution of particular scalars for the indeterminate scalar x_i, becoming reducible.—The structure of the algebra depends in a most intimate way upon its characteristic equation.

2. The definition of associativity leads at once to the theorem that if the latent regions of any faciend or right-handed multiplier,—or simply right multiplier,—be determined, then every facient or left multiplier projects each of these regions into itself. Further, the full effect of every left multiplier can be determined when the internal structure of these latent regions is known.

3. The units and all numbers of the algebra are expressible linearly in terms of certain ideal or auxiliary units called *associative units*, represented in the *Theory* p. 261, by λ_{ijk}. An associative unit may often itself be a unit of the algebra. This happens in the case of group algebras. The third subscript, k, is the *weight* of the associative unit. The aggregate of numbers of which each term has the weight zero form a sub-algebra, since the weight of a product is the sum of the weights of its factors. A sub-algebra of this kind was called by CARTAN * *semi-simple*, his case being such that if λ_{ij0} belongs to it, then λ_{ji0} also belongs. The present writer prefers to call such an algebra or sub-algebra *matric*. It is to be shown that *a group algebra is matric*, that is, its units may all be taken to be of the form λ_{rso}, and such that if λ_{rso} is a unit, λ_{sro} is also a unit. The converse is not true, as may be seen by considering that a matrix of order n, which may be represented as a *quadrate* algebra, does not determine a group of order n^2. †

The immediate problem will now be taken up.

4. *If, in any algebra, a region $\{\theta_i\}$ is such that for each number belonging to the region we have the equation $\theta_i(\psi - g_i) = 0$, ψ being a given number, then the region $\{\theta_i\}$ is free from semilatent regions of ψ, and the form of any left number of the algebra ϕ_i is $\Sigma a_{rso}\lambda_{rso}$ plus terms which annul $\{\theta_i\}$.*

For, in this case the integers ‡ m_r, m_s, etc., all become $= 1$. Hence the weight t must be zero to satisfy the conditions $t < m_r$, $t \equiv m_r - m_s$.

5. *If, for one number ϕ_i' of the region $\{\theta_i\}$, which has m dimensions, let us suppose, we have $\theta_i\phi_i' = \theta_i$ whatever number of that region θ_i may be; and if all the numbers ϕ_i'', $\cdots$, $\phi_i^{(m)}$, independent of ϕ_i' and each other, but belong-*

* *Les Groupes Bilinéaires et les Systèmes de Nombres Complexes*, Annales de la Faculté de Sciences de Toulouse, vol. 12 (1898), p. 57.

† At least a group in the ordinary sense. If the definition of group were extended so as to include cases in which the product of any two operators gave a third operator multiplied by a scalar factor, the case would be different. A matrix does determine a group of order n^3, however.

‡ *Theory*, p. 265, § 4, et seq., p. 273, § 6.

ing to the region, give $\theta_i \phi_i^{(r)} = 0$ $(r = 2 \cdots m)$, *then the algebra of that region is definable by the units* λ_{r10}, $r = 1, \cdots, m$, $\phi_i^{(r)} = \lambda_{rio}$.

6. If there are other regions of m dimensions of similar character, then each is definable by m units $\lambda_{q_i ro}(i = 1, \cdots, m)$. If any one of the first set can multiply one of this set giving a product which does not vanish, as

$$\lambda_{t10} \cdot \lambda_{q_i ro} = \lambda_{tro},$$

then $\lambda_{q_i ro}$ must have the form λ_{1ro}, and by multiplication of the two sets we find the second set must be representable by $\lambda_{sro}(s = 1, \cdots, m)$. If there are m numbers of the form λ_{iio} each determining a region thus, the entire set of numbers so determined is representable by $\lambda_{tuo}(t, u = 1, 2, \cdots, m)$. There are then m^2 such units λ, forming a quadrate algebra.

7. From the properties of the operators of the group, we have for any analogous unit of the algebra, as e_r, whose $m + 1$ power equals itself, the equations:

$$e_r^m \cdot a = a = a \; e_r^m.$$

In this equation a is any number of the algebra. Therefore as a multiplier, e_r has a characteristic equation

$$(e_r^m - 1) \cdot = 0 = \cdot (e_r^m - 1).$$

If ω is a primitive mth root of unity, this equation may be written in the form

$$(e_r - 1)(e_r - \omega) \cdots (e_r - \omega^{m-1}) \cdot = 0.$$

Since the ground is of order $n = qm$, and since this equation contains each factor only to the first degree, it follows *e_r has n latent roots in m sets of q identical roots, and each distinct root has a latent region of q dimensions and no semilatent* regions of any species.*

8. It follows that if we construct the number

$$\begin{aligned} f_r &= (e_1 - 1)(e_1 - \omega^{-1}) \cdots (e_1 - \omega^{-(r-1)})(e_1 - \omega^{-(r+1)}) \cdots (e_1 - \omega) \\ &= 1 + \omega^r e_1 + \omega^{2r} e_1^2 + \cdots + \omega^{(m-1)} e_1^{m-1}, \end{aligned}$$

it will give us, when used as a right multiplier on all numbers of the algebra, the region $\{c_r\}$, for every number of which,

$$c_r \cdot f_r = c_r, \qquad c_r \cdot f_s = 0 \qquad (r + s),$$

and also

$$c_r \cdot e_1 = \omega^r c_r.$$

The m numbers $f_1, f_2, \cdots, f_m$ will thus serve to divide the ground into m

* WHITEHEAD, *Universal Algebra*, vol. 1, p. 258. For a higher type of semi-latency compare *Theory*, p. 271–272.

exclusive regions, each corresponding to a root of e_1. If the numbers f were used as left multipliers, the same would be true, although in general the regions would be made up differently. For any operator of the group a similar statement holds.

9. Let a set of independent generators of a group be $e_1, e_2, \cdots, e_c$. Starting with any one of the generators, say e_1, of period or multiplicity m_1, $e_1^{m_1} - 1 = 0$, and putting ω for a primitive m_1th root of unity, let us form the numbers $f_{11}, f_{12}, \cdots, f_{1m_1}$, which give us the m_1 distinct latent regions of $(\ )\cdot e_1$. For convenience, let us call the number for any multiplier whatever which annuls the whole ground of the algebra except the latent region of a certain root g of the multiplier, a *latent* of the multiplier, corresponding to the root g. By a theorem in matrices* the multiplier is the sum of the products of the roots into their corresponding *latents*, when there are no semi-latent regions. We may then call $f_{11}, \cdots, f_{1m_1}$ the latents of e_1. Each is of the form

$$f_{1r} = \frac{1}{m_1}(1 + \omega^r e_1 + \omega^{2r} e_1^2 + \cdots + \omega^{(m_1-1)r} e_1^{m_1-1}) \quad (r = 1, 2, \cdots, m_1).$$

These numbers are the products of all the latent factors except the one corresponding to the root ω^{-r}, divided by the corresponding factors with ω^{-r} substituted for e_r. These latents of e_1 divide the whole ground of the algebra into regions $\{\theta_r\}$, such that for any number in one of these regions, as θ_r,

$$\theta_r \cdot f_{1r} = \theta_r,$$

and

$$\theta_r \cdot f_{1s} = 0 \qquad (s \neq r).$$

Necessarily $f_{1r}\cdot$ is itself included in the region $\{\theta_r\}$, for

$$f_{1r} \cdot f_{1r} = f_{1r}.$$

Any number of the region $\{\theta_r\}$ must have the form

$$pf_{1r},$$

where p is some product of the generators of the group. Since the region $\{\theta_r\}$ is of n/m_1 dimensions, there are n/m_1 independent numbers of the form just given, and as $e_2\phi$ does not vanish for any number of the algebra, $e_2 f_{1r}$, as also $e_3 f_{1r}$, $e_2 e_3 f_{1r}$, $e_3 e_2 f_{1r}$, etc., are all to be found among the numbers of $\{\theta_r\}$. Any number of the algebra as left multiplier must project these regions into themselves,† so that we have for any number ϕ and any region $\{\theta_r\}$,

$$\phi \cdot \{\theta_r\} = \{\theta_r\}.$$

We may then state the following theorem:

* TABER, *Theory of Matrices*, American Journal of Mathematics, vol. 12 (1890), p. 378.

† *Theory*, p. 268.

A first separation of the numbers of the algebra into mutually exclusive regions is effected by multiplying the entire ground of the algebra on the right by the latents of $(\ )\cdot e_1$, *these latents being numbers of the algebra depending only on the generator* e_1. *Every number of the algebra as a left multiplier is equivalent to the sum of partial multipliers in terms of* λ_{ijk}, *corresponding to these regions and each in effect operative only on its corresponding region.*

10. Suppose next that the n independent numbers just found are taken as defining the ground. Then for any one of them, as $e_2 f_{1r}$, we must have, within the region to which $e_2 f_{1r}$ belongs, as many roots, equal or unequal, as the region has dimensions. Let the latents of $(\ )\cdot e_2 f_{1r}$ be formed, represented by f_{1rs}. The regions outside $\{\theta_r\}$, as $\{\theta_t\}$ give $\{\theta_t\} f_{1rs} = 0$.* Then the numbers f_{1rs} divide $\{\theta_r\}$ into mutually exclusive regions, just as f_{1r} did the whole ground. Letting r and s take all values which give independent numbers, we have the whole ground of the algebra divided more minutely into regions which are exclusive, and also for any one of which, say $\{\theta_{rs}\}$, we have, ϕ being any number of the algebra,

$$\phi\{\theta_{rs}\} = \{\theta_{rs}\}.$$

It is to be noted that the number of distinct roots of $e_2 f_{1r}$ may differ from that of $e_2 f_{1r'}$.

It is also evident that $\phi(\ )$ must be made up of multipliers (possibly ideal only and expressible only in terms of the λ's) each operative on a single region $\{\theta_{rs}\}$, and also, in case $e_2 f_{1r}$ have roots with semi-latent regions (which, it will appear later, it has not), so constituted as to be still commutative with $(\ )\cdot e_2 f_{1r}$. This being the case, $\phi\cdot(\ )$ will be necessarily commutative with $(\ )\cdot e_2$, since it is commutative with $(\ )e_1$ and $(\ )f_{1r}$. We have therefore the theorem:

The latents of $(\ )e_2 f_{1r}$, $(r = 1, 2, \cdots m_1)$, *give a second separation of the ground into exclusive regions, and any number* ϕ *is the sum of multipliers operative only on these regions.*

11. In the region $\{\theta_{rs}\}$ there must be an expression $e_3 f_{1rs}$. If we form the latents of $(\ )e_3 f_{1rs}$, let them be f_{1rst}; then these expressions will divide the ground of the algebra into exclusive regions as before. We may so proceed with each generator, building up latents for each combination, each set of latents dividing the whole ground into smaller regions.

A repetition of the process of separation for a set of independent generators produces a separation of the ground into mutually exclusive regions, and any facient number of the ground is the sum of parts each operative in only one of these regions.

It is to be noted that this process may be applied to any algebra defined by means of generators, whatever the equations of the generators.

*Since $(\ )e_2 f_{1r}$ projects all such regions into $\{\theta_r\}$.

12. Now if any left multiplier ϕ projects the latent regions of $(\ )e_1$ into themselves, and those of $(\ )e_2 f_{1r}$ into themselves, then ϕ projects the latent regions of $(\ )e_2$ into themselves, and likewise those of $(\ )e_2^x e_1^y$ into themselves. Hence when we have used each independent generator in the manner indicated, we shall have ϕ so constituted in terms of the λ's that it projects each latent region of each generator used as a right multiplier into itself, and also projects the right latent regions of any combination of such generators into themselves.* Since no further conditions are imposed then on the associative units, it follows that any new latent would simply give us the same regions. In fact if we had started with more generators than were independent, we should discover this fact by reaching eventually a division into regions $\{E_{qr}\}$, each of which is such that any expression chosen from it has the entire region $\{E_{qr}\}$ for the latent region of its one latent root.† These ultimate regions are reached when we have built up the latents so as to include each generator. Let any such region be $\{E_{qr}\}$ determined by $(\ )F_r$, as above. The totality of the defining numbers of all these regions also define the algebra. $\{E_{qr}\}$ cannot vanish under right-hand multiplication by every number, but for some one at least must give itself as result. This multiplier is $(\ )\cdot F_r$. Also F_r is one of the numbers of $\{E_{qr}\}$, since at least one number of $\{E_{qr}\}$ must give $\{E_{qr}\}$ as the result of right multiplication into the whole domain (otherwise the process would not have terminated).

If now $\cdot F$ is any latent with properly chosen scalar coefficients we know from the theory of matrices that $(\cdot F)^2 = \cdot F$. Hence since $\cdot F^2 - \cdot F = 0$, and since F has but one root in its own region, having the root zero everywhere else, it follows that for each number E_{qr}, we must have for F_r the equation

$$E_{qr} \cdot F_r = E_{qr}.$$

Also $E_{qs} \cdot F_r = 0$, and $F_r^2 \cdot = F_r$.

From this equation, and because any left multiplier leaves each region invariant, it follows that in any region of m dimensions we must have m axes of $F_r(\ )$, and these may be taken to be the m numbers E_{qr} defining the region. Hence

$$F_r \cdot E_{qr} = E_{qr} \text{ or } 0.$$

Similarly for any other region E_{pt}:

$$F_r \cdot E_{pt} = E_{pt} \text{ or } 0.$$

If E_{pt} is a latent axis of F_r it cannot be a latent axis of any other latent F_s, for if $F_r E_{pt} = F_{pt}$, then $F_s E_{pt} = F_s F_r E_{pt} = 0$.

* *Theory*, p. 273, § 6.

† *Example:* Part 2, § 3. The regions E are (λ_{11}), (λ_{22}), (λ_{33}), $(\lambda_{44}, \lambda_{54}, \lambda_{64})$, $(\lambda_{45}, \lambda_{55}, \lambda_{65})$, $(\lambda_{46}, \lambda_{56}, \lambda_{66})$. If $e_3 = e_1 e_2$ appeared as generator also, $e_3 \lambda_{qr}$ is already in $\{\lambda_{qr}\}$.

The non-zero-axes of each latent F_r, are zero-axes of every other latent F_s, and the numbers E_{qr} can be idemfactorial only for one latent on the left F_q, and one on the right F_r, or $E_{qr} = F_q E_{qr} F_r$.

13. The only numbers E which can have unity for root must be of the form $E_{rr} = F_r$. There can be only one in each region; for, if two, let the second be E'_{rr}. Then $E_{rr} \cdot E_{rr} = E_{rr}$, $E_{rr} \cdot E'_{rr} = E_{rr}$, therefore

$$E_{rr}(E_{rr} - E'_{rr}) = F_r(E_{rr} - E'_{rr}) = E_{rr} - E'_{rr} = 0.$$

Hence $E'_{rr} = E_{rr}$.

Each region therefore is a case of the theorem of § 5 above, and the defining elements may be written in the form

$$\lambda_{qr0}.$$

Since $F_r \cdot$ has the form E_{rr}, $F_r = \lambda_{rr0}$.

14. Again, since $F_r \cdot (\ )$ has only one latent axis for the root unity in any region, it follows that in some other region there are one or more such axes. Hence one such must have the form

$$\lambda_{rs0},$$

and as all the λ's of form λ_{qr0} will multiply this, we find that for each form in λ_{qr0} there is a form in λ_{ts0}. Hence also λ_{sr0} must appear among the forms λ_{qr0}. Therefore there is no second form λ'_{rs0} multiplicable by λ_{rr0}, else it would give two forms λ_{ss0} and λ'_{ss0} which is impossible. Further there is no form λ_{ts0} not included in the forms $\lambda_{qr0} \cdot \lambda_{rs0}$, else it would give $\lambda_{ts0} \cdot \lambda_{sr0} = \lambda_{tr0}$, and there is no such form. Finally, therefore, each latent axis of $F_r = \lambda_{rr0}$, corresponding to the root unity, lies in a different region $\{E_{ri}\}$, and hence the regions combine according to theorem of § 6. We may then state the final theorem of the investigation:

THEOREM. *The numbers of the algebra are linearly expressible in terms of a set of semi-simple terms of the form λ_{qro}, which are determined by operating on every number of the algebra by the latents $F_q \cdot (\ )$, $(\ ) F_r$. The scalar coefficients of the products must be determined so as to satisfy the equations $\lambda_{qro} \cdot \lambda_{rso} = \lambda_{qso}$. These terms collect in sets of μ_1^2, μ_2^2, $\cdots$, μ_p^2, where $n = \mu_1^2 + \mu_2^2 + \cdots + \mu_p^2$. Each set determines an independent quadrate algebra, the group-algebra being the sum of these sub-algebras, that is, a semi-simple or matric algebra. The general equation of any number of the algebra,*

$$\phi = \Sigma x_{ij} \lambda_{ijo},$$

is

$$|x_{r_1 s_1} - \phi| \cdot |x_{r_2 s_2} - \phi| \cdot \cdots = 0,$$

the μ_i^2 elements of the i-th determinant being made up of the x's of the i-th sub-algebra.

15.* It is evident, as POINCARÉ pointed out,† that, since the operators of the group may be put into s mutually exclusive conjugate classes, if we consider the corresponding numbers of the algebra, then σ_a, the sum of all numbers in the a conjugate class, must be commutative with every number of the algebra. Hence σ_a must take the form

$$\sigma_a = \Sigma \cdot a_j \lambda_{ii0}^{(j)} \qquad (i=1, \cdots, \mu_i\,;\ j=1, \cdots, s).$$

Since these sums σ are independent of each other, if we multiply them by proper scalars and add them, we can find s independent numbers of the algebra which are commutative with every number of the algebra. *Each of these numbers* ϕ_k, $k=1, \cdots, s$, *must be of the form* $\Sigma\lambda_{ii0}^{(k)}$. For, evidently $\Sigma_{\lambda ii0}^{(k)}$ is commutative with every number, and hence is linearly expressible in terms of the σ's; and no number $\Sigma\lambda_{ii0}^{(k)}$ can be broken up in the process of addition used. Therefore, $s=p$, or *there are as many quadrate algebras as there are conjugate classes.* The numbers σ form an abelian algebra.

16. The numbers ϕ_k are the numbers which satisfy the equations

$$\sigma_a \phi_k = g \cdot \phi_k \qquad (a=1, \cdots, p),$$

where g is some scalar coefficient. That is, they are the common latent regions of all the σ's. Also since $\phi_k = \Sigma\lambda_{ii0}^{(k)}$, we may isolate the k-th quadrate algebra by operating on every number of the algebra by ϕ_k; the results will be linearly expressible in terms of μ_k^2 independent numbers, and these numbers will readily yield the units $\lambda_{ij0}^{(k)}$, of the quadrate. This process reduces the labor of computation decidedly.

17. Further, the number μ_k^2 is the multiplicity of the root unity of ϕ_k, so that if n_k is the nullity of the number ϕ_k, its general equation must be

$$(\phi_k - 1)^{\mu_k^2} \phi_k^{n_k} = 0 \qquad (\mu_k^2 + n_k = n).$$

PART 2. APPLICATION TO CERTAIN GROUPS.

1. *Abelian Groups.* An abelian group gives terms of only one form λ_{rr0}. For if any term λ_{rs0} existed, there would be expressions not commutative with all other expressions. It follows that *every abelian group of order n gives the same group algebra.*‡

As a particular case, consider the algebra of the abelian group defined by the generators e_1, e_2, subject to the equations $e_1^4 = 1 = e_2^2$, $e_1 e_2 = e_2 e_1$. Let ω be a primitive fourth root of unity. Let

$$f_{1i} = \tfrac{1}{4}(1 + \omega^{i-1} e_1 + \omega^{2(i-1)} e_1^2 + \omega^{3(i-1)} e_1^3) \qquad (i=1, 2, 3, 4).$$

* §§ 15, 16, 17 were added to the paper May 30, 1904.

† Loc. cit.

‡ It should be remembered that the field of coefficients is the scalar continuous field of numbers.

Whence $e_2 f_{11} = \frac{1}{4} e_2 (1 + e_1 + e_1^2 + e_1^3)$, $(e_2 f_{11})^2 = f_{11}$, $(e_2 f_{11})^3 = (e_2 f_{11})$. Therefore the equation of $\cdot e_2 f_{11}$ is

$$\cdot (e_2 f_{11})(e_2 f_{11} - 1)(e_2 f_{11} + 1) = 0.$$

This gives, with similar equations for $e_2 f_{1i}$,

$$F_{2i} = \tfrac{1}{2}(f_{1i} - e_2 f_{1i}), \qquad F_{2i-1} = \tfrac{1}{2}(f_{1i} + e_2 f_{1i}) \quad (i = 1, 2, 3, 4).$$

Hence the algebra is defined by

$$\lambda_{rr} \qquad (r = 1, \cdots, 8).$$

We find easily

$$e_1 = \lambda_{11} + \lambda_{22} + \omega^3 \lambda_{33} + \omega^3 \lambda_{44} + \omega^2 \lambda_{55} + \omega^2 \lambda_{66} + \omega \lambda_{77} + \omega \lambda_{88},$$
$$e_2 = \lambda_{11} - \lambda_{22} + \lambda_{33} - \lambda_{44} + \lambda_{55} - \lambda_{66} + \lambda_{77} - \lambda_{88}.$$

The correspondence between the forms for this group of order 8 and the cyclic group of order 8, is interesting. If σ is a primitive 8th root of unity, the generator of the cyclic group is

$$e = \Sigma \sigma^{r-1} \lambda_{rr} \qquad (r = 1, \cdots, 8).$$

Whence

$$e = \tfrac{1}{2}[1 + \sigma + e_2(1 - \sigma)] e_1^3,$$

and conversely

$$e_2 = e^4, \qquad e_1 = \tfrac{1}{2}[1 - \sigma + e^4(1 + \sigma)]\, e^3.$$

Of course the groups are distinct, although the group algebras are identical.

2. *The Dihedron Groups.* The generators are e_1, e_2, with equations $e_1^m = 1 = e_2^2$, $e_2 e_1 = e_1^{m-1} e_2$. Let $\omega^m = 1$. There are two cases, according as m is (1) odd, (2) even:

In the *first case*, let

$$f_{1i} = \frac{1}{m}(1 + \omega^{i-1} e_1 + \omega^{2(i-1)} e_1^2 + \cdots + \omega^{-(i-1)} e_1^{-1}) \quad (i = 1, \cdots, m).$$

Hence

$$F_1 = \tfrac{1}{2}(f_{11} + e_2 f_{11}), \qquad F_2 = \tfrac{1}{2}(f_{11} - e_2 f_{11}),$$
$$F_{2+r} = f_{1r+1} \qquad (r = 1, \cdots, m-1).$$

The forms are therefore

$$\lambda_{11}, \lambda_{22}, \lambda_{2r-1,\,2r-1}, \lambda_{2r-1,\,2r}, \lambda_{2r,\,2r-1}, \lambda_{2r,\,2r} \quad (r = 2, \cdots, (m+1)/2).$$

Whence

$$e_1 = \lambda_{11} + \lambda_{22} + \omega^{-1} \lambda_{33} + \omega \lambda_{44} + \omega^{-2} \lambda_{55} + \omega^2 \lambda_{66} + \cdots + \omega^{-\frac{m-1}{2}} \lambda_{mm} + \omega^{\frac{m-1}{2}} \lambda_{m+1,\,m+1},$$
$$e_2 = \lambda_{11} - \lambda_{22} + \lambda_{34} + \lambda_{43} + \lambda_{56} + \lambda_{65} + \cdots + \lambda_{mm+1} + \lambda_{m+1\,m}.$$

In the *second case*, we find the algebra to be defined by

$$\lambda_{11}, \lambda_{22}, \lambda_{33}, \lambda_{44}, \lambda_{2r-1,\,2r-1}, \lambda_{2r-1,\,2r}, \lambda_{2r,\,2r-1}, \lambda_{2r,\,2r} \quad (r = 3, \cdots, m/2 + 1).$$

These give

$$e_1 = \lambda_{11} + \lambda_{22} - \lambda_{33} - \lambda_{44} + \Sigma\omega^{-(r-2)}\lambda_{2r-1,\,2r-1} + \Sigma\omega^{r-2}\lambda_{2r,\,2r},$$
$$e_2 = \lambda_{11} - \lambda_{22} + \lambda_{33} - \lambda_{44} + \Sigma(\lambda_{2r-1,\,2r} + \lambda_{2r,\,2r-1}).$$

3. *The Tetrahedral Group of Order* 12. The generators are e_1, e_2, with the equations $e_1^3 = 1$, $e_2^2 = 1$, $e_2e_1^2 = e_1e_2e_1e_2$. Let $\omega^3 = 1$. Then

$$f_{11} = \tfrac{1}{3}(1 + e_1 + e_1^2), \quad f_{12} = \tfrac{1}{3}(1 + \omega e_1 + \omega^2 e_1^2), \quad f_{13} = \tfrac{1}{3}(1 + \omega^2 e_1 + \omega e_1^2).$$

The equations of e_2f_{11}, e_2f_{12}, e_2f_{13}, are

$$e_2f_{11}(e_2f_{11} - 1)(e_2f_{11} + \tfrac{1}{3}) = 0, \qquad e_2f_{12}(e_2f_{12} - 1)(e_2f_{12} + \tfrac{1}{3}) = 0,$$
$$e_2f_{13}(e_2f_{13} - 1)(e_2f_{13} + \tfrac{1}{3}) = 0.$$

Therefore we have

$$\lambda_{11} = \tfrac{1}{4}(f_{11} + 3f_{11}e_2f_{11}), \quad \lambda_{22} = \tfrac{1}{4}(f_{12} + 3f_{12}e_2f_{12}), \quad \lambda_{33} = \tfrac{1}{4}(f_{13} + 3f_{13}e_2f_{13}),$$
$$\lambda_{44} = \tfrac{3}{4}(f_{11} - f_{11}e_2f_{11}), \quad \lambda_{54} = \tfrac{3}{2}f_{12}e_2f_{11}, \quad \lambda_{64} = \tfrac{3}{2}f_{13}e_2f_{11},$$
$$\lambda_{45} = \tfrac{3}{2}f_{11}e_2f_{12}, \quad \lambda_{55} = \tfrac{3}{4}(f_{12} - f_{12}e_2f_{12}), \quad \lambda_{65} = \tfrac{3}{2}f_{13}e_2f_{12},$$
$$\lambda_{46} = \tfrac{3}{2}f_{11}e_2f_{13}, \quad \lambda_{56} = \tfrac{3}{2}f_{12}e_2f_{13}, \quad \lambda_{66} = \tfrac{3}{4}(f_{13} - f_{13}e_2f_{13}),$$

the generators are therefore

$$e_1 = \lambda_{11} + \omega^2\lambda_{22} + \omega\lambda_{33} + \lambda_{44} + \omega^2\lambda_{55} + \omega\lambda_{66},$$
$$e_2 = \lambda_{11} + \lambda_{22} + \lambda_{33} - \tfrac{1}{3}\lambda_{44} + \tfrac{2}{3}\lambda_{54} + \tfrac{2}{3}\lambda_{64} + \tfrac{2}{3}\lambda_{45} - \tfrac{1}{3}\lambda_{55} + \tfrac{2}{3}\lambda_{65} + \tfrac{2}{3}\lambda_{46} + \tfrac{2}{3}\lambda_{56} - \tfrac{1}{3}\lambda_{66}.$$

4. *The Octahedral Group of Order* 24. The generators are e_1, e_2, with the equations $e_1^4 = 1 = e_2^3$, $e_2^2 = e_1e_2e_1$. Let $\omega^4 = 1$, and put

$$e_{r2r} = f_{1r}e_2f_{1r}$$
$$= \tfrac{1}{16}(1 + \omega^{r-1}e_1 + \omega^{2(r-1)}e_1^2 + \omega^{3(r-1)}e_1^3)e_2(1 + \omega^{r-1}e_1 + \omega^{2(r-1)}e_1^2 + \omega^{3(r-1)}e_1^3),$$
$$e_{rs} = f_{1r}e_2f_{1s} \qquad (r, s = 1, 2, 3, 4)$$

Then the equations of e_{121}, e_{222}, e_{323}, e_{424}, are

$$e_{121}^2(e_{121} - 1)(2e_{121} + 1) = 0, \qquad e_{222}(2e_{222} + \omega)(2e_{222} - \omega) = 0,$$
$$e_{323}^2(e_{323} - 1)(2e_{323} + 1) = 0, \qquad e_{424}(2e_{424} + \omega)(2e_{424} - \omega) = 0,$$

whence

$$\lambda_{11} = \tfrac{1}{3}(2 \cdot e_{121}^3 + e_{121}^2), \qquad \lambda_{33} = \tfrac{8}{3}(e_{121}^3 - e_{121}^2), \qquad \lambda_{34} = \frac{2}{\sqrt{-3}}e_{321},$$

$$\lambda_{22} = \tfrac{1}{3}(2 \cdot e_{323}^3 + e_{323}^2), \qquad \lambda_{44} = \tfrac{8}{3}(-e_{323}^3 + e_{323}^2), \qquad \lambda_{43} = \frac{2}{\sqrt{-3}}e_{123},$$

$$\lambda_{55} = f_{11} + e_{121} - 2e_{121}^2, \quad \lambda_{56} = (1-\omega)e_{122}, \quad \lambda_{57} = (1+\omega)e_{124},$$
$$\lambda_{65} = (1-\omega)e_{221}, \quad \lambda_{66} = \omega e_{222} - 2e_{222}^2, \quad \lambda_{67} = 2e_{221}e_{124},$$
$$\lambda_{75} = (1+\omega)e_{421}, \quad \lambda_{76} = 2e_{421}e_{122}, \quad \lambda_{77} = -\omega e_{424} - 2e_{424}^2,$$
$$\lambda_{88} = f_{13} + e_{323} - 2e_{323}^2, \quad \lambda_{89} = (1+\omega)e_{322}, \quad \lambda_{8a} = (1-\omega)e_{324},$$
$$\lambda_{98} = (1+\omega)e_{223}, \quad \lambda_{99} = -e_{222} - 2e_{222}^2, \quad \lambda_{9a} = 2e_{223}e_{324},$$
$$\lambda_{a8} = (1-\omega)e_{423}, \quad \lambda_{a9} = 2e_{423}e_{322}, \quad \lambda_{aa} = \omega e_{424} - e_{424}^2.$$

These give for the generators

$$e_1 = \lambda_{11} - \lambda_{22} + \lambda_{33} - \lambda_{44} + \lambda_{55} + \omega^3\lambda_{66} + \omega\lambda_{77} - \omega\lambda_{88} + \omega^3\lambda_{99} + \omega\lambda_{aa},$$
$$e_2 = \lambda_{11} + \lambda_{22} - \tfrac{1}{2}\lambda_{33} + \tfrac{1}{2}\sqrt{-3}\,\lambda_{34} + \tfrac{1}{2}(1+\omega)\lambda_{56} + \tfrac{1}{2}(1-\omega)\lambda_{57} + \tfrac{1}{2}(1-\omega)\lambda_{89}$$
$$+ \tfrac{1}{2}(1+\omega)\lambda_{8a} + \tfrac{1}{2}\sqrt{-3}\,\lambda_{43} - \tfrac{1}{2}\lambda_{44} + \tfrac{1}{2}(1+\omega)\lambda_{65} - \tfrac{1}{2}\omega\lambda_{66} + \tfrac{1}{2}\lambda_{67}$$
$$+ \tfrac{1}{2}(1-\omega)\lambda_{98} + \tfrac{1}{2}\omega\lambda_{99} + \tfrac{1}{2}\lambda_{9a} + \tfrac{1}{2}(1-\omega)\lambda_{75} + \tfrac{1}{2}\lambda_{76} + \tfrac{1}{2}\omega\lambda_{77}$$
$$+ \tfrac{1}{2}(1+\omega)\lambda_{a8} + \tfrac{1}{2}\lambda_{a9} - \tfrac{1}{2}\omega\lambda_{aa}.$$

5. *A group of order* 16, defined by the generators e_1, e_2, e_3, with the equations

$$1 = e_1^4 = e_3^2, \quad e_1^2 = e_2^2, \quad e_1e_2 = e_2e_1, \quad e_1e_3 = e_3e_1^3, \quad e_2e_3 = e_3e_2^3.$$

Let $\omega^4 = 1$. The equations of

$$e_{121} = f_{11}e_2f_{11}, \quad e_{222} = f_{12}e_2f_{12}, \quad e_{323} = f_{13}e_2f_{13}, \quad e_{424} = f_{14}e_2f_{14},$$

are

$$(e_{121}^2 - f_{11}) = 0, \quad (e_{222}^2 + f_{12}) = 0, \quad (e_{323}^2 - f_{13}) = 0, \quad (e_{424}^2 + f_{14}) = 0.$$

Hence

$$f_{111} = \tfrac{1}{2}(f_{11} + e_{121}), \quad f_{121} = \tfrac{1}{2}(f_{11} - e_{121}), \quad f_{212} = \tfrac{1}{2}(f_{12} - \omega e_{222}),$$
$$f_{222} = \tfrac{1}{2}(f_{12} + \omega e_{222}), \quad f_{313} = \tfrac{1}{2}(f_{13} + e_{323}), \quad f_{323} = \tfrac{1}{2}(f_{13} - e_{323}),$$
$$f_{414} = \tfrac{1}{2}(f_{14} + \omega e_{424}), \quad f_{424} = \tfrac{1}{2}(f_{14} - \omega e_{424}),$$

setting

$$e_{11311} = f_{111}e_3f_{111}, \quad e_{12312} = f_{121}e_3f_{121}, \text{ etc.},$$

we find

$$e_{11311}^2 - f_{111} = 0, \quad e_{12312}^2 - f_{121} = 0, \quad e_{21321}^2 = 0, \quad e_{22322}^2 = 0,$$
$$e_{31331}^2 - f_{313} = 0, \quad e_{32332}^2 - f_{323} = 0, \quad e_{41341}^2 = 0, \quad e_{42342}^2 = 0,$$

therefore

$$\lambda_{11} = \tfrac{1}{2}(f_{111} + e_{11311}), \qquad \lambda_{22} = \tfrac{1}{2}(f_{111} - e_{11311}),$$
$$\lambda_{33} = \tfrac{1}{2}(f_{121} + e_{12312}), \qquad \lambda_{44} = \tfrac{1}{2}(f_{111} - e_{12312}),$$
$$\lambda_{55} = f_{212}, \qquad \lambda_{56} = e_{21321},$$
$$\lambda_{65} = e_{22322}, \qquad \lambda_{66} = f_{222},$$
$$\lambda_{77} = \tfrac{1}{2}(f_{313} + e_{31331}), \qquad \lambda_{88} = \tfrac{1}{2}(f_{313} - e_{31331}),$$
$$\lambda_{99} = \tfrac{1}{2}(f_{323} + e_{32332}), \qquad \lambda_{aa} = \tfrac{1}{2}(f_{323} - e_{32332}),$$
$$\lambda_{bb} = f_{414}, \qquad \lambda_{bc} = e_{41341},$$
$$\lambda_{cb} = e_{42342}, \qquad \lambda_{cc} = f_{424}.$$

$$e_1 = \lambda_{11} + \lambda_{22} + \lambda_{33} + \lambda_{44} - \omega\lambda_{55} - \omega\lambda_{66} - \lambda_{77} - \lambda_{88} - \lambda_{99} - \lambda_{aa} + \omega\lambda_{bb} + \omega\lambda_{cc}.$$
$$e_2 = \lambda_{11} + \lambda_{22} - \lambda_{33} - \lambda_{44} + \omega\lambda_{55} - \omega\lambda_{66} + \lambda_{77} + \lambda_{88} - \lambda_{99} - \lambda_{aa} - \omega\lambda_{bb} + \omega\lambda_{cc}.$$
$$e_3 = \lambda_{11} - \lambda_{22} - \lambda_{33} + \lambda_{44} + \lambda_{56} + \lambda_{65} - \lambda_{77} + \lambda_{88} - \lambda_{99} + \lambda_{aa} + \lambda_{bc} + \lambda_{cb}.$$

Part 3. Relation to the Theories of Group Determinants, Group Characters, and Groups Defined by Finite Groups.

1. We consider a group of order n with the n operators e_r $(r = 1, \cdots, n)$ and write the general number of its group-algebra in terms of the corresponding units e_r,

$$\phi = \Sigma x_r e_r.$$

If we also use for x_k the notation x_{ij} in case $e_i e_j = e_k$, and the notation $x_{ij^{-1}}$ in case $e_i e_j^{-1} = e_k$, we find by multiplying ϕ into each unit e_r $(r = 1, \cdots, n)$, that ϕ satisfies the equation:

$$f(\phi) \equiv \begin{vmatrix} x_{11^{-1}} - \phi, & x_{12^{-1}}, & \cdots, & x_{1n^{-1}} \\ x_{21^{-1}}, & x_{22^{-1}} - \phi, & \cdots, & x_{2n^{-1}} \\ \cdots & \cdots & \cdots & \cdots \\ x_{n1^{-1}}, & x_{n2^{-1}}, & \cdots, & x_{nn^{-1}} - \phi \end{vmatrix} = 0,$$

of degree n, the general equation of ϕ. The *characteristic* equation satisfied by ϕ is usually of much lower degree, whose factors all appear however in the equation $f(\phi) = 0$. The determinant $f(0)$ is the absolute term of the general equation of ϕ. This determinant may also be written, by shifting the rows and columns, in the form $\pm |x_{ij}| (i, j = 1, \cdots, n)$. The first form of the determinant is the *group-determinant* of Frobenius, * who studied the factorisation of

* Berliner Sitzungsberichte: *Über Gruppencharaktere*, 1896, pp. 985–1021; *Über die Primfactoren der Gruppendeterminante*, 1896, pp. 1343–1382; *Über die Darstellung der endlicher*

it and gave the theory of certain coefficients involved in its expansion which he called *group-characters*.

2. If we suppose that for every unit e we substitute its value in terms of the λ's we have $\phi = \Sigma a_{ijk}\lambda_{ijk}$. As shown above, the λ's appear in sets of μ_r^2. The coefficients a are linear homogeneous functions of the x's of § 1. The characteristic equation of ϕ will consist of the shear factors corresponding to the sets of λ's, each shear factor being a determinant and appearing to the first degree only, since there are no λ's of weight more than zero.* These shear factors appear in the general equation of ϕ, which is of degree n, to the same power as their width, since in the *frame*,† each factor of order μ_r appears μ_r times on the diagonal.‡ In previous discussions relating to this subject the general equation of ϕ has been treated,§ but no mention has been made of the reduced equation. It is readily seen that the determinant of ϕ is the product of the determinants of the shear factors, each to a degree equal to its width. The determinant factors are the *irreducible factors* of FROBENIUS.

To make the matter still clearer, let us consider the group of order 6, defined by the generators $e_1^3 = 1 = e_2^2$, $e_2 e_1 = e_1^2 e$. Let $\omega^3 = 1$. Having a dihedron group, we obtain as the six units

$$e_1 = \lambda_{11} + \lambda_{22} + \omega^2\lambda_{33} + \omega\lambda_{44}, \qquad e_2 = \lambda_{11} - \lambda_{22} + \lambda_{34} + \lambda_{43},$$
$$e_3 = \lambda_{11} + \lambda_{22} + \omega\lambda_{33} + \omega^2\lambda_{44}, \qquad e_4 = \lambda_{11} - \lambda_{22} + \omega^2\lambda_{34} + \omega\lambda_{43},$$
$$e_6 = \lambda_{11} + \lambda_{22} + \lambda_{33} + \lambda_{44}, \qquad e_5 = \lambda_{11} - \lambda_{22} + \omega\lambda_{34} + \omega_2\lambda_{43}.$$

Therefore

$$\begin{aligned}\phi = {} & \lambda_{11}(x_1 + x_2 + x_3 + x_4 + x_5 + x_6) + \lambda_{22}(x_1 + x_3 + x_6 - x_2 - x_4 - x_5) \\ & + \lambda_{33}(x_6 + \omega x_3 + \omega^2 x_1) + \lambda_{34}(x_2 + \omega x_5 + \omega^2 x_4) \\ & + \lambda_{43}(x_2 + \omega x_4 + \omega^2 x_5) + \lambda_{44}(x_6 + \omega x_1 + \omega^2 x_3).\end{aligned}$$

The characteristic equation of ϕ is

$$(x_6 + x_1 + x_2 + x_3 + x_4 + x_5 - \phi)(x_6 + x_1 + x_3 - x_2 - x_4 - x_5 - \phi)$$
$$\begin{vmatrix} x_6 + \omega x_3 + \omega^2 x_1 - \phi & x_2 + \omega x_5 + \omega^2 x_4 \\ x_2 + \omega x_4 + \omega^2 x_5 & x_6 + \omega x_1 + \omega^2 x_3 - \phi \end{vmatrix} = 0.$$

Gruppen durch lineare Substitutionen, 1897, pp. 994–1015; 1899, pp. 482–500; *Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen*, 1898, pp. 501–515; *Über die Composition der Charaktere einer Gruppe*, 1899, pp. 330–339; *Über die Charaktere der Symmetrie und Alternirenden Gruppen*, 1900, pp. 516–534; 1901, pp. 303–315.

DICKSON, *Elementary Exposition of Frobenius' Theory of Group-Characters and Group-Determinants*, Annals of Mathematics, vol. 4 (1902), pp. 25–49.

* *Theory*, pp. 264, 275, 277.

† *Theory*, p. 265.

‡ *Theory*, pp. 275, 276.

§ See citations above.

The general equation has these same factors, the determinant however appearing to degree 2. The equation may be written also

$$f(\phi) = \begin{vmatrix} x_6-\phi & x_1 & x_2 & x_3 & x_4 & x_5 \\ x_3 & x_6-\phi & x_4 & x_1 & x_5 & x_2 \\ x_2 & x_5 & x_6-\phi & x_4 & x_1 & x_3 \\ x_1 & x_3 & x_5 & x_6-\phi & x_2 & x_4 \\ x_4 & x_2 & x_3 & x_5 & x_6-\phi & x_1 \\ x_5 & x_4 & x_1 & x_2 & x_3 & x_6-\phi \end{vmatrix} = 0,$$

the determinant being $f(0)$.

It is obvious that any matric algebra, whether group algebra or not, has a general equation which contains shear factors that belong to the characteristic equation each with an exponent equal to some order; but these exponents in the *characteristic* equation are all unity. For example, quaternions reduces to a form expressible in four λ's, having a characteristic equation of degree 2, and a general equation which is the square of the reduced. This property is due to the absence in the frame of the algebra of any terms off the main diagonal. That is, if λ_{rs0} appears, then λ_{sr0} also appears. This theorem may also be proved for group-algebras by proving that if ϕ is any given number of such an algebra, then if ψ be every number of the algebra, it is impossible that $\phi\psi$ can have only zero for a root for all values of ψ. This is equivalent to saying that if λ_{rs0} occur in ϕ, then λ_{sr0} must also occur in some ψ, and that $\lambda_{rst}, t \neq 0$, cannot occur. If we put $\phi = \Sigma x_r e_r$, $\psi = \Sigma y_s e_s$, e_t being one of n units, then we have

$$\phi\psi = \Sigma x_r y_s \cdot e_{rs} \qquad (e_{rs} = e_r \cdot e_s).$$

Now for $\phi\psi$ to have only zero roots for every value of y_r, the coefficients of the equation of $\phi\psi$ must all vanish, leaving $(\phi\psi)^n = 0$. But each coefficient reduces to a sum of products of determinants of the x's multiplied by corresponding determinants of the y's. Each such determinant in the x's must vanish then, the y's being arbitrary; that is, all minors of the determinant of ϕ must vanish. But the coefficient of $(\phi\psi)^{n-1}$ cannot thus vanish unless each x vanishes. Hence every expression ϕ has a multiplier which produces a term λ_{ii0}, and hence if λ_{rs0} is such a number ϕ, there must also be λ_{sr0} in the algebra, and it is a matric algebra.

3. Turning our attention to the equation of ϕ in its general form, we may write it, as any matrix equation may be written,

$$\phi^n - m_1\phi^{n-1} + m_2\phi^{n-2} \cdots \pm m_n = 0.$$

The coefficient m_n is the determinant of the matrix. The coefficients m_1, m_2,

$\cdots$, m_n, are respectively the sums of all minors of orders $1, 2, \cdots, n-1$, whose main diagonal is that of the determinant m_n. Thus, in the example above we have the following table of coefficients for the six numbers ϕ:

ϕ	m_1	m_2	m_3	m_4	m_5	m_6
e_0	6	15	20	15	6	1
e_1	0	0	2	0	0	1
e_2	0	3	0	3	0	1
e_3	0	0	2	0	0	1
e_4	0	3	0	3	0	1
e_5	0	3	0	3	0	1

Confining our attention to the coefficient m_1, we notice that each coefficient m_1 is the sum of what we may call *partial coefficients* of the nature of m_1, one from each quadrate. Thus $m_1 =$

	$\{\lambda_{11}\}$		$\{\lambda_{22}\}$		$\{\lambda_{33}, \lambda_{34}, \lambda_{43}, \lambda_{44}\}$	
e_0	1	+	1	+	$2 \cdot 2$	$= 6,$
e_1	1	+	1	+	$2(\omega^2 + \omega)$	$= 0,$
e_2	1	−	1	+	$2 \cdot 0$	$= 0,$
e_3	1	+	1	+	$2(\omega + \omega^2)$	$= 0,$
e_4	1	−	1	+	$2 \cdot 0$	$= 0,$
e_5	1	−	1	+	$2 \cdot 0$	$= 0.$

These *partial coefficients* from the different regions are the *group characters* of FROBENIUS.* It is to be noticed that they are the same for sets of operators, viz., for sets of conjugate operators. Thus for

	(11)	(22)	(34)
e_0	$m_1' = 1,$	$m_1'' = 1,$	$m_1''' = 2,$
e_1, e_3	$m_1' = 1,$	$m_1'' = 1,$	$m_1''' = \omega^2 + \omega = -1,$
e_2, e_4, e_5	$m_1' = 1,$	$m_1'' = -1,$	$m_1''' = 0.$

This is to be expected from the theory of matrices. For, in any case, if ϕ, χ belong to the same ground, ϕ and $\chi\phi\chi^{-1}$ have the same equation, and in each exclusive region have the same coefficients. This means of course that any

* Cf. DICKSON, *loc. cit.*

operator and its conjugates must have the same *characters*. In the example given,

$$e_3 = e_2 e_1 e_2^{-1}, \qquad e_4 = e_1^2 e_2 e_1^{-2}, \qquad e_5 = e_1 e_2 e_1^{-1}.$$

4. Within the limits of this paper it is impossible to re-develop the whole theory of group-characters, but it is evident that such development is quite possible on the basis of this theory, and indeed is quite simple. The relations of the coefficients $m_1, m_2, \cdots, m_n$ of any expression ϕ to those of $e_1, \cdots, e_n$ have been developed in papers read before this society some time ago.*

5. Reverting now to the equation

$$\phi = \Sigma x_r e_r \qquad (r=1, \cdots, n),$$

it is obvious that if

$$\psi = \Sigma y_s e_s \qquad (s=1, \cdots, n),$$

then

$$\phi\psi = \Sigma\Sigma x_{rs-1} y_s e_r \qquad (r, s=1, \cdots, n).$$

Consequently $\phi\psi$ belongs to the algebra, and if the coefficients of $\phi, \psi, \cdots$ run through all scalar values, real or imaginary, the expressions $\phi, \psi, \cdots$ form a continuous group. Since these equations are equivalent to a continuous group of linear homogeneous substitutions, this gives a basis for BURNSIDE'S theory of continuous groups defined by finite groups.† The theory may be developed from the preceding results.

6. BURNSIDE'S theory of continuous groups defined by finite groups has been generalized by DICKSON,‡ in that the coefficients x_r, y_s, are taken as numbers (marks) in any field F whatsoever. The management of this problem develops the need of certain canonical forms which are essentially the units λ_{ij} above. If the coefficients of any linear associative algebra are restricted§ to any field F, we may nevertheless develop the theorems of such algebra, and this is particularly true of the group-algebras belonging to such fields. In fact, the determination of the group-algebra of any finite group with respect to any field seems to be a necessary common basis for the diverse problems mentioned.

December 1, 1903.

---

* Bulletin of the American Mathematical Society, vol. 5 (1899), p. 381. These papers are unpublished. It may be noted that FROBENIUS' method determines the width of the exclusive regions of λ's but does not determine $e_1, \cdots, e_n$ in terms of the λ's. This method determines λ_{ij_0} in terms of $e_1, \cdots, e_n$, whence the inverse problem becomes easy.

† Proceedings of the London Mathematical Society, vol. 29 (1898), pp. 207–224, 546–565.

‡ *On the Group defined for any given Field by the Multiplication Table of any Given Finite Group*, Transactions of the American Mathematical Society, vol. 3 (1902), pp. 285–301. Also certain special cases, Proceedings of the London Mathematical Society, vol. 35 (1902), pp. 68–80. Also *Groups defined for a General Field by the Rotation Groups*, University of Chicago Decennial Publications, vol. 9 (1902), pp. 35–51.

§ This generalization was first made by DICKSON: *Definitions of a Linear Associative Algebra by Independent Postulates*, Transactions of the American Mathematical Society, vol. 4 (1903), pp. 21–26.

A SYSTEM OF AXIOMS FOR GEOMETRY*

BY

OSWALD VEBLEN

Contents.

CHAPTER I. *The axioms and their independence.*
Introductory statement of the axioms . . . . . § 1
Categorical and disjunctive systems . . . . . § 2
Independence proofs and historical remarks on axioms IX–XII. § 3–6
Finite systems proving the independence of I–VIII . . . . § 7–14
CHAPTER II. *General properties of space.*
Definition and properties of line, plane, space . . . . . § 1–3
Generalizations of order. Regions. . . . . § 4
Continuity . . . . . § 5
Parallel lines . . . . . § 6
CHAPTER III. *Projective and metric geometry.*
Ideal elements defined independently of XI and XII . . . . § 1–2
Fundamental theorems of projective geometry . . . . . § 3–6
Definition of congruence relations . . . . . § 7–8
The axiom system as categorical. . . . . § 9

CHAPTER I.

THE AXIOMS AND THEIR INDEPENDENCE.

§ 1. *Statement of the axioms.*

Euclidian geometry is a system of propositions codifying in a definite way† our spatial judgments. A system of axioms for this geometry is a finite number of these propositions satisfying the following two conditions:

1. Every proposition of euclidian geometry can be deduced from the axioms.
2. No axiom can be deduced from the other axioms.

* Presented to the Society April 11, 1903. Received for publication March 3, 1904.

† By no means the only way. Cf. BOLYAI, LOBATCHEWSKY, VERONESE.

Thus an axiom differs from any other proposition of the science, as thus codified, in that it is *unproved.**

The propositions brought forward as axioms in this paper are stated in terms of a class of elements called "points" and a relation among points called "order"; they thus follow the trend of development inaugurated by PASCH,† and continued by PEANO‡ rather than that of HILBERT§ or PIERI.‖¶ All other geometrical concepts, such as line, plane, space, motion, are defined in terms of point and order. In particular, the congruence relations are made the subject of definitions** rather than of axioms. This is accomplished by the aid of projective geometry according to the method first given analytically by CAYLEY and KLEIN.†† The terms "point" and "order" accordingly differ from the other terms of geometry in that they are *undefined.*

The axioms are twelve in number; they presuppose only the validity of the operations of logic and of counting (ordinal number).‡‡

AXIOM I. There exist at least two distinct points.

AXIOM II.§§ If points A, B, C are in the order ABC, they are in the order CBA.

AXIOM III. If points A, B, C are in the order ABC, they are not in the order BCA.

---

* Many writers replace the word "axiom" by "unproved proposition" or "primitive proposition."

† M. PASCH, *Vorlesungen über neuere Geometrie*, Leipzig, Teubner, 1882.

‡ G. PEANO, *I principii di geometria*, Turin, 1889; *Sui fondamenti della geometria*, Rivista di Matematica, vol. 4 (1894), pp. 51–59.

§ D. HILBERT, *Grundlagen der Geometrie*, Leipzig, 1899. The references are to the English translation by E. J. Townsend, Open Court Publishing Co., Chicago, 1902.

‖ M. PIERI, *Della geometria elementare come sistema ipotetico deduttivo. Monografia del punto e del moto*, Memorie della Reale Accademia delle Scienze di Torino (2), vol. 49 (1899), pp. 173–222. For other references to PIERI, see footnote to § 2, chap. III.

¶ Particular theorems or axioms derived from these and other writers I have acknowledged in footnotes or in §§ 3–14 of this chapter. I wish to express deep gratitude to Professor E. H. MOORE, who has advised me constantly and valuably in the preparation of this paper, and also to Messrs. N. J. LENNES and R. L. MOORE, who have critically read parts of the manuscript.

** A definition is an agreement to substitute a simple term or symbol for more complex terms or symbols. On the distinction between definitions and axioms see A. PADOA, Bibliothèque du Congrès International de Philosophie, III, "Logique et Histoire des Sciences" (1901), p. 309; PEANO, ibid., p. 279; E. H. MOORE, Bulletin of the American Mathematical Society (2), vol. 9 (1903), p. 402. O. VEBLEN, Monist, vol. 13, no. 2 (January, 1903), pp. 303–9.

†† A. CAYLEY, *Sixth Memoir on Quantics*, Collected Works, vol. 2, p. 56 (see also CAYLEY's note, Ibid., p. 605).

F. KLEIN, Mathematische Annalen, vol. 4 (1870), p. 573.

J. THOMAE, *Geometrie der Lage*, Halle, 1873.

E. B. WILSON, *Projective and Metric Geometry*, Annals of Mathematics, vol. 5, p. 145 (1904).

‡‡ In particular, the distinctness of A and B in the order ABC is a theorem.

§§ Mr. R. L. MOORE suggests that "If A is a point, B is a point, C is a point" would be a more rigorous terminology for the hypotheses of II, III, IV, inasmuch as we do not wish to imply that any two of the points are distinct.

AXIOM IV. If points A, B, C are in the order ABC, then A is distinct from C.

AXIOM V. If A and B are any two distinct points, there exists a point C such that A, B, C are in the order ABC.

DEF. 1. The *line* AB ($A \neq B$) consists of A and B and all points X in one of the possible orders ABX, AXB, XAB. The points X in the order AXB constitute the *segment* AB. A and B are the *end-points* of the segment.

AXIOM VI. If points C and D ($C \neq D$) lie on the line AB, then A lies on the line CD.

AXIOM VII. If there exist three distinct points, there exist three points A, B, C not in any of the orders ABC, BCA, or CAB.

DEF. 2. Three distinct points not lying on the same line are the *vertices* of a *triangle* ABC, whose *sides* are the segments AB, BC, CA, and whose *boundary* consists of its vertices and the points of its sides.

AXIOM VIII. If three distinct points A, B, and C do not lie on the same line, and D and E are two points in the orders BCD and CEA, then a point F exists in the order AFB and such that D, E, F lie on the same line.

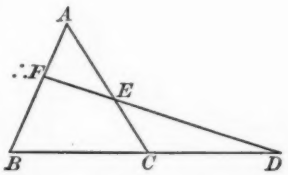

FIG. 1.

DEF. 5. A point O is *in the interior of* a triangle if it lies on a segment, the end-points of which are points of different sides of the triangle. The set of such points O is *the interior* of the triangle.

DEF. 6. If A, B, C form a triangle, the *plane* ABC consists of all points collinear with any two points of the sides of the triangle.

AXIOM IX. If there exist three points not lying in the same line, there exists a plane ABC such that there is a point D not lying in the plane ABC.

DEF. 7. If A, B, C, and D are four points not lying in the same plane, they form a *tetrahedron* $ABCD$ whose *faces* are the interiors of the triangles ABC, BCD, CDA, DAB (if the triangles exist)* whose *vertices* are the four points, A, B, C, and D, and whose *edges* are the segments AB, BC, CD, DA, AC, BD. The points of faces, edges, and vertices constitute the *surface* of the tetrahedron.

DEF. 8. If A, B, C, D are the vertices of a tetrahedron, the space $ABCD$ consists of all points collinear with any two points of the faces of the tetrahedron.

* Without this phrase, the definition might be thought to involve some hypothesis about the non-collinearity of the vertices of the tetrahedron. In K'_{III} (§ 12) there is a tetrahedron of only three faces.

AXIOM X. If there exist four points neither lying in the same line nor lying in the same plane, there exists a space $ABCD$ such that there is no point E not collinear with two points of the space, $ABCD$.

AXIOM XI. If there exists an infinitude of points, there exists a certain pair of points AC such that if $[\sigma]$* is any infinite set of segments of the line AC, having the property that each point which is A, C or a point of the segment AC is a point of a segment σ, then there is a finite subset $\sigma_1, \sigma_2, \cdots, \sigma_n$ with the same property.

AXIOM XII. If a is any line of any plane α there is some point C of α through which there is not more than one line of the plane α which does not intersect a.

§ 2. *Categorical system. Independence of axioms in general.*

Inasmuch as the terms *point* and *order* are undefined one has a right, in thinking of the propositions, to apply the terms in connection with any class of objects of which the axioms are valid propositions. It is part of our purpose however to show that there is *essentially only one* class of which the twelve axioms are valid. In more exact language, any two classes K and K' of objects that satisfy the twelve axioms are capable of a one-to-one correspondence such that if any three elements A, B, C of K are in the order ABC, the corresponding elements of K' are also in the order ABC. Consequently any proposition which can be made in terms of points and order either is in contradiction with our axioms or is equally true of all classes that verify our axioms. The validity of any possible statement in these terms is therefore completely determined by the axioms; and so any further axiom would have to be considered redundant.† Thus, if our axioms are valid geometrical propositions, they are sufficient for the complete determination of euclidian geometry.

A system of axioms such as we have described is called *categorical*, whereas one to which it is possible to add independent axioms (and which therefore leaves more than one possibility open) is called *disjunctive*.‡ The categorical property of a system of propositions is referred to by HILBERT in his "Axiom der Vollständigkeit," which is translated by TOWNSEND into "Axiom of Completeness." E. V. HUNTINGTON,§ in his article on the postulates of the real number system, expresses this conception by saying that his postulates are sufficient for the *complete definition* of essentially a single assemblage. It would probably be better to reserve the word *definition* for the substitution of one

* $[e]$ denotes a set or class of elements, any one of which is denoted by e alone or with an index or subscript.

† Even were it not deducible from the axioms by a finite number of syllogisms.

‡ These terms were suggested by PROFESSOR JOHN DEWEY.

§ E. V. HUNTINGTON, *A Complete Set of Postulates for the Theory of Absolute Continuous Magnitude*, Transactions of the American Mathematical Society, vol. 3, p. 364 (1902).

symbol for another, and to say that a system of axioms is categorical if it is sufficient for the complete *determination* of a class of objects or elements.

An example of a disjunctive set of axioms is furnished as soon as we leave out any one of the axioms in the set above. For instance, all the first eleven axioms are satisfied if the class of *points* is taken to consist of all the points interior to a sphere and *order* as referring to the usual relation of order among these points. Axiom XII is evidently not a valid proposition of this class. The first eleven axioms (excluding XII) therefore can refer to at least two essentially different classes and so form a disjunctive system.

The example just given serves also to show that axiom XII satisfies the second of the conditions named in § 1 for a proposition to be an axiom. It cannot be logically deduced from axioms I–XI; in technical language, it is *independent*.

In the following sections, besides some remarks on the history and formal peculiarities of the axioms, the independence of each of the twelve axioms is to be proved in the manner just indicated. That is, for axiom N ($N = \text{I}, \text{II}, \cdots, \text{XII}$) a class of objects K_N will be exhibited which satisfies each of the axioms except N and for which N is not satisfied. Therefore if axiom N were omitted the system of axioms would be disjunctive and so the validity of N is not determined by the other axioms.

§ 3. *Parallels. Axiom XII.*

The parallel axiom was the first whose independence was seriously studied. Its history* is so well known that I need only mention the names, BOLYAI, LOBATCHEWSKY, RIEMANN, BELTRAMI, CAYLEY, KLEIN. The form in which it is here stated is due to C. BURALI-FORTI.†

The class of points interior to a sphere has been given in § 2 as K_{XII}.

The questions whether axiom XII would still be sufficient if stated for only one plane instead of for any plane, or for only one line of any plane instead of for any line of any plane can both be answered in the negative. The class K'_{XII}, consisting of all the points on a certain side of a certain plane π, is such that in at least one plane, namely, any plane parallel to π, there is only a single parallel to any line through any point. In the same system, in any plane, there is at least one line, namely, the line parallel to π, to which there is only one parallel through any point.

§ 4. *Continuity. Axiom XI.*

The proposition here adopted as the continuity axiom is referred to by

* For bibliography, see G. B. HALSTED, American Journal of Mathematics, vol. 7, p. 264 (1878); also American Mathematical Monthly, vol. 8, pp. 216–230 (1901).

† C. BURALI-FORTI, *Les postulats pour la géométrie d'Euclide et de Lobatchewsky*, p. 264, Verhandlungen des Ersten Internationalen Mathematiker Congresses, Leipzig, 1898.

SCHOENFLIES * as the HEINE-BOREL theorem. So far as I know, it was first stated formally (as a theorem of analysis rather than of geometry) by BOREL † in 1895 but is involved in the proof of the theorem of uniform continuity given by HEINE ‡ in 1871. The idea of its equivalence with the Dedekind cut axiom was the result of a conversation with Mr. N. J. LENNES.

The independence of XI is well known. XI and its consequence, the so-called Archimedean axiom, § have been discussed by VERONESE, ‖ STOLZ, ¶ LEVI-CIVITA, ** HILBERT, †† and DEHN. ‡‡

That theorem 38, which shows the existence of at least one parallel to a given line, cannot be proved without recourse to XI is shown by K_{XI} of which the points are the rational points of an ordinary coördinate geometry, viz., points whose coördinates are all rational numbers, and also the points at infinity collinear with at least two rational points. To define order, consider the plane σ through the points $(\pi, 0, 0)$, $(0, \pi^2, 0)$, $(0, 0, \pi^3)$ where π is the ludolphian constant. This plane contains no point of K_{XI}. *Points A, B, C, of K_{XI} are in the order ABC if, in the ordinary geometry, A, B, C are collinear and A, C are separated by B and the point in which the line AB meets the plane σ.* The axioms I–X are satisfied and every two complanar lines meet.

K_{XI} is determined categorically by a system of twelve axioms, the first ten of which are identical with I–X, and the eleventh of which is

XI′. On a certain line there are three points that are harmonically related to every point of the line.

and the twelfth of which is

XII′. Every two complanar lines meet in a point.

On the basis of these axioms the same proof of the fundamental theorem of pro-

---

* A. SCHOENFLIES, *Bericht über die Mengenlehre*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 8 (1898), p. 51.

† É. BOREL, Annales de l'École Normale Supérieure (3), vol. 12 (1895), p. 51. It is stated by BOREL for a numerable set of segments.

‡ E. HEINE, *Die Elemente der Functionenlehre*, Crelle, vol. 74 (1872), p. 188.

§ Cf. O. STOLZ, *Zur Geometrie der Alten, insbesondere über ein Axiom des Archimedes*, Mathematische Annalen, vol. 22 (1883).

‖ G. VERONESE, *Fondamenti di geometria, a più dimensioni e a più specie di unità rettilinee*, Padua, 1891. German translation by Schepp, Leipzig, 1894.

¶ O. STOLZ, *Ueber das Axiom des Archimedes*, Mathematische Annalen, vol. 39 (1891), p. 107.

** T. LEVI-CIVITA, Memorie della Reale Accademia dei Lincei Roma, vol. 7 (1898), pp. 91–96, 113–131.

†† D. HILBERT, l. c., § 12 and also, *Ueber den Satz von der Gleichheit der Basiswinkel im gleichschenkligen Dreieck*, Proceedings of the London Mathematical Society, vol. 35 (1902), p. 50.

‡‡ M. DEHN, *Die Legendre'schen Sätze über die Winkelsumme im Dreieck*, Mathematische Annalen, vol. 53 (1900), p. 404.

§§ A test of completeness for the axiomatic analysis of a mathematical science would be the question whether for every theorem one can specify a subset of the axioms, sufficient and individually indispensable for its proof. In the present system the answer to this question is affirmative in the cases that I have investigated.

jective geometry can be made as in § 6, chapter III because theorem 67 is an evident consequence of XI′.

§ 5. *Tridimensionality. Axiom* X.

As K_X may be taken the usual four-dimensional geometry. The axiom equivalent to X in the systems of PASCH and HILBERT is:

"If two planes α, β have a point A in common, then they have at least a second point B in common." *

This is essentially theorem 25, § 3, chapter II. PEANO's axiom XVI in the *Principii* is nearly the same as ours; namely, "if A and B are such that the segment AB meets a plane π, then for any point X, either the segment AX or the segment BX meets π."

§ 6. *Relation of plane and space geometry. Axiom* IX.

The class of points K_{IX} is the set of points in an ordinary plane subject to the usual order relations. The non-desarguesian "geometries" of HILBERT † and MOULTON ‡ may be enumerated respectively as K_{IX}^{H} and K_{IX}^{M}. They show the essential dependence of the Desargues theorem (62, chap. III) and harmonic properties (§ 5, chap. III) of the plane upon axiom IX.

This axiom, not stated explicitly by PASCH, is number XV (page 23) in PEANO's *Principii*, and is part of I7 in HILBERT's system. For the suggestion to state this axiom for only a *single* plane as well as VII for only a single triad of points I am indebted to Professor MOORE.

§ 7. *Significance and construction of finite independence proofs.*

The independence proofs of the first eight axioms can all be exhibited by means of finite classes of elements or points. That such independence proofs are not possible for IX–XII is a consequence of theorem 12, based on I–VIII, that every line contains an infinitude of points. The finiteness of $K_I, \cdots, K_{VIII}$ shows conversely that every one of the first eight axioms is essential to the proof of theorem 12. It also brings into relief an important difference between our system of axioms and the systems based on RIEMANN's concept of space as fundamentally a number-manifold. By the method of RIEMANN, the axioms serve to distinguish space from all possible number-manifolds, by the other method they distinguish it from all systems of objects of any kind.

* The form quoted is HILBERT's II6.

† D. HILBERT, *Foundations of Geometry*, p. 74, § 23.

‡ F. R. MOULTON, *A simple non-desarguesian plane geometry*, Transactions of the American Mathematical Society, vol. 3 (1902), p. 192.

The description of the following tactical systems is preliminary to the exposition of $K_I, \cdots, K_{VIII}$.*

By $S\{3, 2, 5\}$ is denoted the system of ordered triads or permutations:

123, 234, 345, 451, 512	135, 352, 524, 241, 413
321, 432, 543, 154, 215	531, 253, 425, 142, 314

Each ordered pair of elements determines a unique element that precedes it, a unique element that follows it and a unique middle element. All the triads can be obtained from 123, 321, 531, 135 by the cyclic substitution (12345).

By $S[3, 2, 7]$ is denoted the *triadic system* of seven vertically printed triads:

0	1	2	3	4	5	6
1	2	3	4	5	6	0
3	4	5	6	0	1	2

It has the property 1st that every pair of elements lies in a unique triad and 2nd every pair of triads has a unique common element. $S[3, 2, 7]$ is invariant under the well-known group G^7_{168} of order 168 with generators,

$$S_1 = (0123456),$$
$$S_2 = (0)(124)(365),$$
$$S_3 = (0)(1)(3)(26)(45),$$
$$S_4 = (0)(1)(3)(25)(46).$$

All the triads are obtained from any one by the cyclic substitution S_1. Notation apart, this is the only triadic system in seven elements.

Analogous to a triadic system is the pentadic system $S[5, 2, 21]$ of twenty-one vertically printed pentads:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	0
6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	0	1	2	3	4	5
8	9	10	11	12	13	14	15	16	17	18	19	20	0	1	2	3	4	5	6	7
18	19	20	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

Every pair of elements lies in one and only one pentad and every two pentads have in common one and only one element. $S[5, 2, 21]$ is invariant under a group G^{21} of order $21 \cdot 20 \cdot 16 \cdot 9 \cdot 2 = 120960$, with the following generators:

* A rich collection of such systems (not, however, including $S[5, 2, 21]$) is to be found in the memoir, *Tactical Memoranda*, I–III, by E. H. Moore, American Journal of Mathematics, vol. 18 (1896), p. 264.

$T_1 = (0, 1, 2, 3. 4, 5, 6, 7, 8, 9, 10, 11, 12. 13, 14, 15, 16, 17, 18, 19, 20),$

$T_2 = (0)(1, 2, 4, 8, 16, 11)(3, 6, 12)(5, 10, 20, 19, 17, 13)(7, 14)(9, 18, 15),$

$T_3 = (0)(1)(2, 9)(7, 19)(6, 8, 18)(12, 11, 16, 4, 15, 3)(5, 14, 17, 10, 20, 13),$

$T_4 = (0)(1)(3, 16)(17, 13)(6, 18, 8)(2, 4, 15, 9, 12, 11)(7, 10, 20, 19, 5, 14),$

$T_5 = (0)(1)(2)(6)(8)(18)(7, 19, 9)(12, 16, 15)(3, 20, 10)(4, 17, 14)(5, 13, 11),$

$T_6 = (0)(1)(2)(3)(8)(9)(16)(12, 15)(13, 17)(6, 18)(7, 19)(5, 14)(4, 11)(10, 20).$

All the pentads are obtained from any one by the cyclic substitution T_1. The group is doubly transitive and indeed such that any three elements not belonging to the same pentad can be transformed into 0, 1, 2.

§ 8. *Triangle transversal. Axiom* VIII.

Axiom VIII was originally stated by PASCH* in a form equivalent to this: "A line lying wholly in a plane and intersecting one side of a triangle of the same plane intersects the perimeter of the triangle in one other point." It was retained by HILBERT as his II 5 in practically the same form. PEANO† made of it two axioms (XIII and XIV) from either of which VIII can be deduced. The statement of the axiom was made considerably weaker than any of its previous forms by Professor MOORE,‡ and the present form is weaker than his.

As the points of K_{VIII} we take the twenty-one elements of $S[5, 2, 21]$. The pentad 0, 1, 6, 8, 18 taken in a definite order determines a system of triads of the type $S\{3, 2, 5\}$. The order of any pentad being defined as that obtained from the above by a cyclic substitution, the twenty-one pentads determine forty-two systems of triads—420 triads in all.

Three points of K_8 are in the order ABC if ABC is one of the 420 *triads just specified.*

Axiom I is valid for K_{VIII} because there are twenty-one points, and axiom II because the order ABC implies a system $S\{3, 2, 5\}$ which by its definition includes the triad CBA. Axiom III is verified because each triad, and indeed each pair, appears in only one pentad and that pentad determines only one order system of the type $S\{3, 2, 5\}$ in which each triad can appear only once. IV is equivalent to the statement that each triad consists of distinct elements. To verify V observe that every pair of elements determines a pentad, and in each pentad by the definition of $S\{3, 2, 5\}$ each pair of elements has a predecessor and a successor.

* M. PASCH, l. c., p. 21.

† G. PEANO, l. c., pp. 18, 21.

‡ E. H. MOORE, *On the projective axioms of geometry*, Transactions of the American Mathematical Society, vol. 3 (1902), p. 147.

A line in K_{VIII} consists of the points of a pentad. VI is a consequence of the proposition that any pair of elements is contained in only one pentad. VII is verified by the points 0, 1, 2 which appear together in no pentad. Since only one point is between any two points, each side of a triangle in K_{VIII} consists of but one point, and thus a plane consists of at most $3 + 3 \times 3 = 12$ points. This verifies IX. X and XII are consequences of the proposition that 0, 1, 2 can be transformed into any non-collinear triad and that every two lines have a point in common. XI is satisfied *vacuously*, i. e., its hypothesis is not fulfilled.

To show that VIII is contradicted, consider the triangle $A = 0, B = 1, C = 3$. Then $D = 13$ and $E = 9$. The point of intersection F of the lines DE and AB is 18, and hence A, B, and F are in the order FAB.

§ 9. *Axiom* VII.

In the class K_{VII} there are five points, 1, 2, 3, 4, 5. *Points A, B, C are in the order ABC if and only if they constitute a triad ABC in the system $S\{3, 2, 5\}$.* The verification of I–VI for K_{VII} was in effect carried out in § 8. VII is negated since all the five points are collinear. VIII–XII are satisfied vacuously.

As K'_{VII} one may take the points of a geometrical line with the usual relations of order.

§ 10. *Axiom* VI.

In the class K_{VI} there are twenty-six points $P_1, P_2, P_3, P_4, P_5, 0, 1, 2, \cdots, 20$. *Points ABC are in the order ABC if and only if they constitute a triad in one of the sets of triads,*

P_1, P_2, P_3, P_4, P_5 *ordered according to* $S\{3, 2, 5\}$,

$0, 1, \cdots, 20$ *ordered according to* $S[5, 2, 21]$ *as in* § 8,

$P_i h P_j$ $\qquad (i, j = 1, \cdots, 5;\ i \neq j;\ h = 0, \cdots, 20)$,

$h P_i k$ $\qquad (h, k = 0, \cdots, 20;\ h \neq k;\ i = 1, \cdots, 5)$.

VI is contradicted in K_{VI} because K_{VI} includes the orders $0P_1 1$ and $1P_1 2$, without containing 012, 120, or 201. Since all the twenty-six points lie on the line $P_1 P_2$ the hypotheses of VIII–XII are not fulfilled. I–V are easily verified.

§ 10. *Axiom* V.

K_V consists of the points, 1 and 2, with the agreement that *points A, B, C are in the order ABC if and only if $A \neq B$, $B \neq C$, $C \neq A$.* I is evidently verified and since there exists no triple of points in the order ABC, V is denied. All the other axioms are satisfied vacuously.

§ 11. *Axiom* IV.

K_{IV} consists of two points, 1 and 2 with the agreement that *points* A, B, C *are in the order* ABC *if* $A = 1, B = 2, C = 1$, *or if* $A = 2, B = 1, C = 2$. IV is evidently contradicted, and I, II, III, V, VI are evidently satisfied. VII–XII are satisfied vacuously.

§ 12. *Axiom* III.

K_{III} consists of two points, 1 and 2 with the agreement that *points* A, B, C *are in the order* ABC *if* $A \neq B$ *and* $B = C$ *or if* $A = B$ *and* $B \neq C$.

K'_{III} consists of seven points $0, 1, 2, 3, 4, 5, 6$, with the agreement that points A, B, C are in the order ABC if they are distinct and constitute a triad of the triadic system $S\,[3, 2, 7]$ (§ 7). In verifying K'_{III} note that a line is a triad of points. The plane 123 consists of the collinear points $4, 5, 0$. The tetrahedron 0124 has as faces the interiors of the triangles 012, 024, 041 (not 124) consisting of the triads 364, 165, 325. Thus the space 0124 includes all seven points.

K''_3 consists of the points of the ordinary projective geometry (see chapter III) with the agreement that points A, B, C are in the order ABC if they are distinct and incident with the same projective line.

§ 13. *Axiom* II.

K_2 consists of two points, 1 and 2, with the agreement that *points* A, B, C *are in the order* ABC *if and only if* $A \neq B$ *and* $B = C$.

§ 14. *Axiom* I.

K_1 consists of one point with the agreement that *points* A, B, C *are in the order* ABC *if and only if* $A \neq B \neq C \neq A$. The other axioms are satisfied vacuously.

CHAPTER II.

General properties of space.

§ 1. *Properties of the line.*

Axiom I. *There exist at least two distinct points.*

Axiom II. *If points* A, B, C *are in the order* ABC, *they are in the order* CBA.

Axiom III. *If points* A, B, C *are in the order* ABC, *they are not in the order* BCA.

Th. 1 (II, III).* If points A, B, C are in the order ABC, they are not in the order CAB.

* The roman numbers in parentheses denote the axioms upon which the proof of the theorem depends. Theorems are occasionally referred to by arabic numbers in parentheses.

Proof. Since the points A, B, C are in the order ABC, that is, for brevity, ABC, then by II CBA, and hence by III the order BAC cannot exist, and therefore by II CAB cannot.

TH. 2 (II, III). The order ABC implies that A is distinct from B and B from C.

Proof. If A were the same as B, the orders ABC and BAC would be the same, contrary to theorem 1. Therefore A is distinct from B. On account of II, the same proof shows that B is distinct from C.

AXIOM IV. *If points A, B, C are in the order ABC, then A is distinct from C.*

Corollary (II, III, IV). The order ABC implies that A, B, and C are distinct points.

AXIOM V. *If A and B are any two distinct points, there exists a point C such that A, B, and C are in the order ABC.*

If A and B stand for the same point we write $A = B$; if for distinct points $A \neq B$.

DEF. 1. The *line* AB ($A \neq B$) consists of A and B and all points X in any one of the orders ABX, AXB, XAB. The points X in the order AXB constitute the *linear segment* AB, or *segment* AB. They are said to lie *between* A and B to be *points of the segment* AB or *interior points* of the segment AB; A and B are *end-points* of the segment. The points X in the order ABX constitute the *prolongation* of the segment AB beyond B, and those in the order XAB the prolongation beyond A. The points of a line are said to *lie on* the line.

In terms of def. 1 the results of the preceding axioms and theorems are:

TH. 3 (I, II, II, IV, V). Every pair of distinct points A and B defines one and only one line AB, and one and only one segment AB. The line or the segment AB is the same as the line or the segment BA. A and B are not points of the segment AB. No two of the three sets of points that (with A and B) constitute the line AB (namely, the segment AB and its two prolongations), have a point in common. There exists at least one point on each prolongation of the segment AB.

It has not been shown as yet that every segment AB contains a point nor that the pair of points AB may not lie on some other line than the line AB.

AXIOM VI. *If points C and D ($C \neq D$) lie on the line AB, then A lies on the line CD.*

TH. 4 (I–VI). Two distinct points lie on one and only one line.

Proof. By theorem 3, it is necessary only to show that if C and D are any two distinct points of a line AB the line CD is the same as the line AB. Suppose first that D is the same as B; we have to show that the line AB is the same as the line BC. Let X be any point of the line $BC (A \neq X \neq B)$.

As A is known to be a point of BC, it follows from VI that B is a point of the line AX. Hence we have one of the orders ABX, AXB or XAB, and therefore X is a point of AB. Similarly any point of AB is shown to be a point of BC. Hence the lines AB and BC are the same. Similar proofs hold if $D = A$ or $C = A$ or $C = B$.

If D and C are both distinct from A and B, we argue that the line AB is the same as BC, which is the same as CD.

Corollary. Two distinct lines can have in common at most one point. Such a common point F is called a point of intersection and the lines are said to *intersect* in F.

AXIOM VII. *If there exist three distinct points there exist three points A, B, C, not in any of the orders ABC, BCA, or CAB.*

TH. 5 (I–VII). If DE is any line, there exists a point F not lying in this line.

Proof. If the line DE contains every point, it would contain the three points A, B, C mentioned in VII. The line AB, by theorem 4, would be the same as DE, and hence AB would contain the point C, contrary to VIII.

DEF. 2. Points lying in the same line are said to be *collinear*. Three distinct non-collinear points, A, B, and C, are the *vertices* of a *triangle* ABC, whose *sides* are the segments AB, BC, CA, and whose *boundary* consists of its vertices and the points on its sides.

AXIOM VIII (*Triangle transversal axiom*). *If three distinct points A, B, C do not lie on the same line, and D and E are two points in the order BCD and CEA, then a point F exists in the order AFB, and such that D, E, F lie on the same line.*

TH. 6 (I–VIII). Between every two distinct points there is a third point.

Proof. Let A and B be the given points (fig. 2). By theorem 5 there is a point E not lying on the line AB. By V points C and D exist, satisfying the order-relations AEC and BCD. Hence, by VIII, F exists in the order AFB.

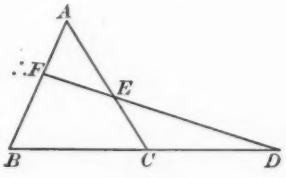

FIG. 2.

TH. 7 (I–VI, VIII). The points D, E, F, of axiom VIII, are distinct, and lie in the order DEF.

Proof. If D, E, F were not distinct, we should by axiom VI have A, B, C collinear. Hence there must be one of the three orders DEF, EFD, FDE, and it is necessary to show EFD and FDE impossible.

1st. Suppose the points were in the order EFD (fig. 3). Consider the triangle DEC (D, E, C being non-collinear by VI), and the orders AEC, DFE. By VIII, a point X exists on the line AF and in the order DXC. But as this point is common to the lines AF and DC, which have B in common, by the corollary of theorem 4, $X = B$. Hence we have the order DBC contrary to hypothesis. Hence DFE is impossible.

2d. Suppose EDF (fig. 4). Consider the triangle EFA (E, F, A being non-collinear by VI) and the orders AEC and EDF. By the same argument as above, we find that B is on the line CD and in the order ABF, which contradicts our hypothesis. Hence EDF is impossible.

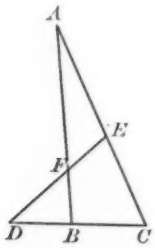

FIG. 3.

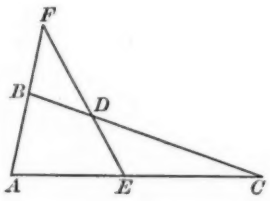

FIG. 4.

TH. 8 (I–VI, VIII). If points A, B, C form a triangle, there is no line that has a point in common with each of the sides AB, BC, CA.

Proof. If the theorem is not verified, we have three collinear points A', B', C', in the three orders $AB'C$, $BC'A$, and $CA'B$. It is evidently sufficient to show the order $A'B'C'$ impossible.

If $A'B'C'$, then A', C', and B would form a triangle; for otherwise A, B, C would be collinear. In connection with the triangle $A'C'B$, consider the order relations $BA'C$, $A'B'C'$. By theorem 7, a point X exists in the order BXC', and $CB'X$. Hence X is the intersection of the lines AB and $B'C$. Hence $X = A$. Hence BAC' contrary to hypothesis.

DEF. 3. If points A, B, C, D are in the orders ABC, ABD, ACD, BCD, they are said to be in the order $ABCD$.

TH. 9 (I–VIII).* To any four distinct points of a line, the notation A, B, C, D, may always be assigned so that they are in the order $ABCD$.

Proof. The proof of this theorem depends on the following six lemmas:

1. If ABC and BCD, then ABD.

By V and theorem 5, there exist points P and O not in the line AB but in the order BPO (Fig. 5). By VIII and theorem 7, since we have the triangle OBC and the orders ABC and BPO there exists a point Q in the orders OQC and APQ. Like-

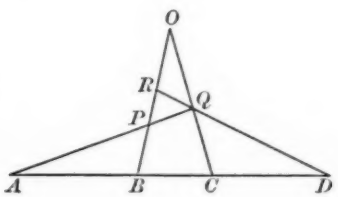

FIG. 5.

* This proposition was given as "Axiom II 4" in HILBERT's *Festschrift* (p. 7). Its redundancy as an axiom of HILBERT's system I, II was proved by E. H. MOORE, *On the projective axioms of geometry*, Transactions of the American Mathematical Society, January, 1902, vol. 3, p. 142–168, 501. A second proof has been given by Mr. R. L. MOORE, cf. p. 98, American Mathematical Monthly, April, 1902.

wise, since we have the triangle OBC and the orders BCD and OQC, there exists a point R in the orders ORB and DQR. Finally, since we have the triangle AQD, and the orders RQD and APQ, there exists a point X in the orders AXD and RPX. But the intersection of the lines AD and RP is B. Hence by the corollary to theorem 4, $X = B$. Hence ABD.

2. If ABC and ABD then either BCD or BDC.

In consequence of VI it is only necessary to show the order CBD impossible. By (5) and V there exist points O and P not collinear with B and C and in the order OCP (fig. 6). Therefore unless our theorem is valid, we have a triangle OCD and the orders OCP and CBD. Hence by VIII and (7), there exists a point Q in the orders OQD and PBQ. Now we have the tri-

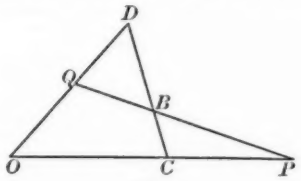

FIG. 6.

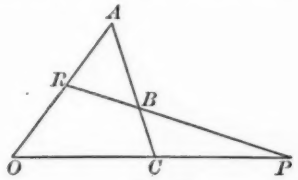

FIG. 7.

angle ACO (fig. 7) and the orders OCP and ABC. Hence a point R exists in the orders PBR and ARO. From the orders PBR and PBQ it follows by VI that R, B, and Q are collinear. But R, B, and Q are points of the sides OA, AD, and DO, of the triangle OAD, and this is in contradiction with theorem 8. Hence CBD is impossible.

3. It follows from 1 and 2 that if ABC and ABD, then either ACD or ADC.

4. If ABD and ACD, then either ABC or ACB.

By theorem 4, we must have either ABC or ACB or BAC. In the last case, from BAC and ACD we could by 1 argue BAD, contrary to hypothesis

5. If ABC and ACD, then BCD.

By theorem 4, if not BCD then BDC or CBD. In the first case, DCA leads by lemma 1 to BCA—a contradiction; and in the second case, CBA leads by lemma 3 to CAD or CDA, either of which contradicts ACD.

6. If ABC and ACD, then ABD.

By lemma 5 we have BCD, and hence ABC leads by lemma 1 to ABD.

We are now ready to complete the proof of theorem 9. Assign the notation A, B, C to three of the points so that they are in the order ABC. The fourth point D will either lie in the order

a) DAB, in which case it follows from 1 that we have $DABC$.

b) ADB, in which case it follows from 5, 6 that we have $ADBC$.

c) ABD, in which case it follows from 2, 1 that we have $ABCD$ or $ABDC$.

In any case the notation can be assigned so that the order is $ABCD$.

DEF. 4. The order $A_1 A_2 \cdots A_i \cdots A_n$ means that the points A_i, A_j, A_k are in the order $A_i A_j A_k$ if $i < j < k$ $(i, j, k = 1, 2, \cdots, n)$.

TH. 10 (I–VIII). To any finite number n, of distinct points of a line, the notation can be so assigned that they are in the order $A_1 A_2 \cdots A_i \cdots A_n$.

Proof. By mathematical induction.

TH. 11 (I–VIII). Any finite set of n distinct points separates a line into $n-1$ segments and two prolongations of segments, no two of which have a point in common.

Proof. It is a consequence of theorem 3 that one point separates a line into two mutually exclusive parts, and two points into three mutually exclusive parts. One point separates a segment into two mutually exclusive segments (9); and a prolongation into a segment and a prolongation. Hence if m points separate a line into $m-1$ segments and two prolongations, adding one point adds one segment, and therefore $m+1$ points divide a line into m segments and two prolongations. Hence by induction from the case $m = 2$ the theorem is proved.

TH. 12 (I–VIII). Between any two points A and B $(A \neq B)$ and also on either prolongation of the segment AB, there exist an infinitude of points.

Proof.* By theorems 6 and 9 it can be proved that if n is any integer there are more than n points X in the order AXB or ABX.

§ 2. *Properties of the plane.*

TH. 13 (I–VIII).† If A, B, and C form a triangle, and D and F exist in the orders BCD and AFB, then E exists in the orders AEC and DEF.

Proof (fig. 8). By V and (9) there exists a point O in the order $OBFA$. Hence by VIII and (7), from the triangle DBF and the orders OBF and BCD, we obtain a point P in the orders OCP and FPD, and from the triangle DAF and the orders OFA, FPD a point Q in the orders OPQ and AQD. By (9), we then have $OCPQ$. Hence in the triangle CAQ we have AQD and CPQ. Hence E exists in the order AEC, and on the line PD, whence by (7) E is in the order DEF.

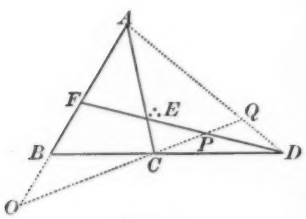

FIG. 8.

TH. 14 (I–VIII). A line that intersects one side of a triangle and a prolongation of another side intersects the third side.

Proof. This simply combines in one statement VIII and theorems 7 and 13.

* That all of the axioms I–VIII are necessary for the proof of this theorem is demonstrated in §§ 7–14, chap. I.

† This proposition has been regarded as an axiom in previous discussions; cf. § 8, chap. I.

DEF. 5. A point O is in the interior of a triangle if it lies on a segment, the end-points of which are points of different sides of the triangle. The set of such points O is the *interior* of the triangle.

TH. 15 (I–VIII). If O is a point collinear with two points M and N of the perimeter of a triangle ABC, a line joining O to any point P of a side of the triangle meets the perimeter in a point Q $(Q \neq P)$.

Proof. This is easily seen if O lies on one of the lines AB, BC, or CA, or if M or N is a vertex; in the latter case, if MON, by joining OA, OB, and OC.

Thus we may suppose that M and N are interior points of AB and AC respectively. In case of the order MNO (figs. 9 and 10), considering the

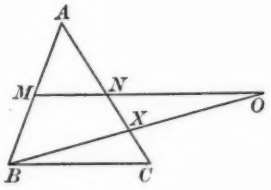

FIG. 9.

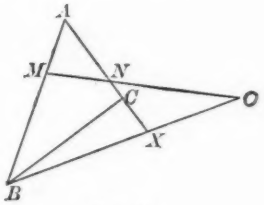

FIG. 10.

triangles OMB, we see that X exists in the orders BXO and ANX, and in view of the order ANC, we have either AXC or ACX. In either case the theorem reduces to theorem 14, in connection with the triangles ABX and BXC.

In case of the order MON (fig. 11), we have by consideration of the triangles MNB and BNC a point X in the order AOX and BXC. Likewise, a point Y in the orders BOY and CYA, and a point Z in the orders COZ and AZB. If P is a point of BC, the theorem follows (14) by consideration of the triangle ABX or BXC. A similar argument holds if P is a point of AB or AC.

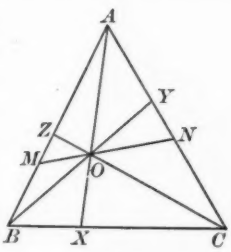

FIG. 11.

DEF. 6. If A, B, C form a triangle, the *plane* ABC consists of all points collinear with any two points of the sides of the triangle.

TH. 16 (I–VIII). Any three non-collinear points lying in a plane determine the plane.

Proof. Let the given plane be ABC. If O is any point of a side AB of the triangle ABC, the points of the plane ABC consist of the points of the lines joining O to the perimeter of ABC. This is a corollary of theorem 15. We prove:

1st, that if A' is any point of the line AB, such that $A' \neq B$, the plane ABC is the same as the plane $A'BC$. In the case of the order $A'AB$ or $AA'B$ (fig. 12), we choose O so that it lies between A or A' and B, and the proposition is an evident consequence of theorem 14. In case of the order ABA', we have just shown that the plane ABC is the same as $AA'C$, which is the same as $BA'C$ or $A'BC$.

2nd, that if C' is any point of the plane ABC not collinear with A and B, the plane ABC is the same as ABC'. Take P between A and B and join

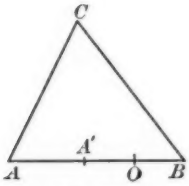

FIG. 12.

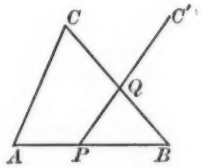

FIG. 13.

PC' (fig. 12), meeting the perimeter of ABC in a point Q, say $Q = C$ or Q on the side BC. By the second part of the proof, ABC is the same as PBC, and hence as PQB, and hence as $PC'B$, and hence as $AC'B$.

3rd, the second step shows that if $A'B'C'$ are any three non-collinear points of the plane, the notation $A'B'C'$ being assigned so that A' is not in BC and B' is not in $A'C$, ABC is the same as $A'BC$, hence the same as $A'B'C$, and hence as $A'B'C'$.

Corollary. A line lying wholly in a plane π and having a point in common with the interior or one side of a triangle which also lies in the plane π meets the perimeter of the triangle in two points.

TH. 17 (I–VIII). A line having two points in common with a plane lies wholly in the plane.

Proof. Let the two points be taken as A and B in defining the plane, ABC. The plane contains the line AB.

Corollary. If two planes have two points in common they have a line in common.

§ 3. *Properties of space.*

AXIOM IX. *If there exist three points not lying in the same line, there exists a plane ABC, such that there is a point D not lying in the plane ABC.*

TH. 18 (I–IX). If ABC is any plane, there exists a point D not in this plane.

Proof. If the plane contained all points it would contain the points A, B,

C mentioned in IX, and would therefore by theorem 16 be the same as the plane ABC of IX, and that plane would contain all points which is contrary to IX.

DEF. 7. If A, B, C, D are four points, not lying in the same plane, they form a *tetrahedron* $ABCD$ whose *faces* are the interiors of the triangles ABC, BCD, CDA, DAB; whose *vertices* are the four points A, B, C, D; and whose *edges* are the six segments AB, BC, CD, DA, AC, BD. A point X is in the *interior* of the tetrahedron if it lies between two points D and E of different faces. The points of the faces, edges, and vertices constitute the *surface* of the tetrahedron.

TH. 19 (I–IX). If any vertex A of a tetrahedron $ABCD$ is joined to an interior point O, the line AO meets the opposite face BCD in a point P lying in the order AOP.

Proof. Since O is an interior point, there exist two points X and Y of the surface in the order XOY (fig. 14). These two points are not both in the same

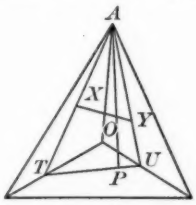

FIG. 14.

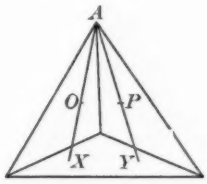

FIG. 15.

face of the tetrahedron, and therefore one of them, X is in a face that has A for a vertex. Join AX, and if Y is in a face that has A for a vertex, join AY also. AX and AY will then meet the perimeter of BCD in two points, T and U. In the triangles XYT and TYU we have the condition of theorem 14. Hence the required point P exists.

If Y is in the face BCD, we have a point T of the perimeter of BCD in the order AXT. Then by theorem 15 U exists on the perimeter of BCD in the order TYU. But in the triangle TXY we again have the hypothesis of theorem 14 and hence a point P in the order TPY. In view of the order TYU, P is in the order TPU.

TH. 20 (I–IX). If any interior point O of a tetrahedron $ABCD$ is joined to another point P of the surface or interior of the tetrahedron, the line OP meets the surface in two points Q and R (where if P is of the perimeter, $P = Q$) lying in the order QOR.

Proof. By theorems 13 and 19, X and Y exist on the interior or perimeter of BCD in the order AOX and APY (fig. 15). Then, by theorem 13, T and U exist on the perimeter of BCD in the orders TXU, and, if $Y \neq U$, TYU. Hence by § 2 OP meets the perimeter of the triangle ATU, and hence the surface of the tetrahedron, in the required points Q and R.

TH. 21 (I–IX). If O is a point in the order MNO with two points M and N of different faces of a tetrahedron $ABCD$, the line joining O to an interior point P of a face of the tetrahedron meets the surface in a point Q, $Q \neq P$.

Proof [I–IX]. 1st (fig.16). Suppose that P is on the same face with M or N. If with M, let X be a point of this face in the order MPX. Then, (14), OP meets the segment NX in a point Y. Y is an interior point of the tetrahedron, and hence the existence of Q follows from theorem 20. A similar argument holds if P is on the same face with N.

2d (fig. 17). Suppose that P is not on the same face with M or N. Let A be the vertex not in the same face with P. Since A is a vertex of every

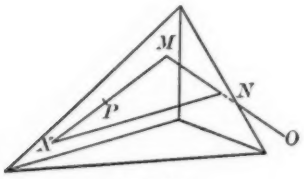

FIG. 16.

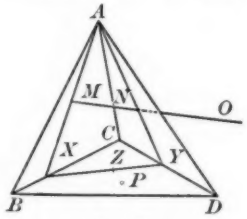

FIG. 17.

face but BCD, on joining AM and AN we obtain X and Y as points of the perimeter of BCD in the orders AMX and ANY. Hence by theorem 15 the line joining O to any point Z in the order XZY meets the perimeter of the triangle AXY in a point W. That PO meets the perimeter now follows from the first part of this proof if O is not in the plane BCD and from § 2 if O is in the plane BCD.

DEF. 8. A *space* $ABCD$, if A, B, C, and D form a tetrahedron, consists of all points collinear with two points of the faces of the tetrahedron.

TH. 22 (I–IX). If two points of a line lie in a space $ABCD$, so does every point of the line.

Proof. If the two points are both complanar with one of the faces of the tetrahedron $ABCD$, apply the results of § 2. If not, let the two points in question be E and F (fig. 18). By theorems 20 and 21, if P is a point of one face, not collinear with E and F, Q and R exist on the surface of $ABCD$, such that Q is on the line PF and R on the line PE, and P, Q, R are not collinear. F and E lie in the plane PQR, and therefore any point of the line X can be joined to two points of the perimeter of the triangle PQR. But every point of PQR is on the surface or in the interior of $ABCD$, and therefore by theorems 20 and 21 every point of the line FE lies in the space $ABCD$.

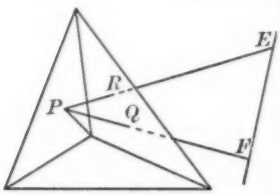

FIG. 18.

TH. 23 (I–IX). Any four non-complanar points of a space define that space.

Proof. Let the given space be $ABCD$, and the four non-complanar points be A', B', C', D'. By theorem 22 every point of the lines $A'B'$ and $A'C'$ belongs to $ABCD$. Hence every point of the plane $A'B'C'$, and hence every point of the space $A'B'C'D'$. Similarly, every point of $ABCD$ belongs to the space $A'B'C'D'$.

Corollary. If three points of a plane lie in a space, so does every point of the plane.

AXIOM X. *If there exist four points neither lying in the same line nor lying in the same plane, there exists a space $ABCD$ such that there is no point E not collinear with two points of the space $ABCD$.*

TH. 24 (I–X). There is but one space.

Proof. By theorem 22 and 23 and axiom X.

TH. 25 (I–X). Two planes that have a point in common have a line in common.

Proof. It is sufficient under the corollary to theorem 17 to show that two planes α and β have two points in common. If O is the given point, let the plane α be defined by points A_1, A_2, A_3, such that O is an interior point of the triangle $A_1A_2A_3$ (this is possible by 16). If B is a point of the second plane not lying in α, let space be defined by the tetrahedron $BA_1A_2A_3$ (fig. 19). If B' is a third point of β the line $B'O$, which lies wholly in β, meets the surface of the tetrahedron (by 24, 20, 21), in another point, B''. If this point B'' is in α, the theorem is proved; if not, join BB''. The line BB'' lies in β and meets one of the lines A_1A_2, A_2A_3, A_3A_1 in a point common to α and β.

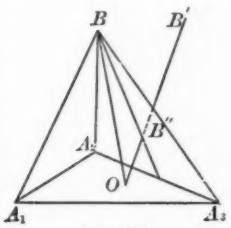

FIG. 19.

§ 4. *Generalizations of order. Regions.*

DEF. 9. The points lying on a system of segments A_1A_2, A_2A_3, $\cdots$, $A_{n-1}A_n$ together with the points (called *vertices*) A_1, A_2, $\cdots$, A_n constitute a *broken line*. If $A_n = A_1$, the broken line, A_1, $\cdots$, A_n is the *boundary of a polygon* of which $A_i (i = 1, \cdots, n-1)$ are the *vertices* and the segments A_iA_{i+1} are the *sides*. A *multiple point* of a polygon or broken line is a point common to a side and a vertex or to two sides or to two vertices. The boundary of a polygon without multiple points is called *simple*.*

DEF. 10. A *region* is a set of points any two of which are points of a broken line composed entirely of points of the set. Two regions, R' and R'', sub-

* A *polygon* is any figure (i. e. class) of sides and vertices, the points of which constitute the "boundary of a polygon." Similar distinctions are made between "angle" and "boundary of an angle," "trihedral angle" and "boundary of a trihedral angle," etc.

sets of the same region, R, are *separated* with respect to R by a set of points $[S]$ if every broken line of R joining a point of R' to a point of R'' contains at least one point of the set $[S]$. $[S]$ is said to *decompose* R into a finite number n of regions if there are n and only n regions $R', R'', \cdots, R^{(n)}$ that include every point of R except $[S]$ and if every pair of regions $R^{(i)}$ and $R^{(k)}$ are separated by $[S]$. Lines, planes, and space are obvious examples of regions as is also the interior of a triangle; the latter is referred to as a *triangular region.*

TH. 26 (I–VIII). Any line decomposes a plane in which it lies into two regions.

Proof. Let A be a point of the line a, and A^+, A^- two points of the plane, α, not of a, and in the order A^+AA^-. It is to be proved: (1) that a region including $\frac{A^+}{A^-}$ and including no point of a does not include $\frac{A^-}{A^+}$; (2) that any region of the plane that includes all points that can be joined to a given point by broken lines not meeting a includes either A^+ or A^-.

The statement (1) is a consequence of the proposition that any broken line of the plane joining A^+ to A^- has a point in common with a. If this were not so a certain broken line $A^+B_1B_2\cdots B_nA^-$ would not intersect a. By the corollary to theorem 16, since A^+B_1, B_1, and B_1B_2 have no point in common with a, neither would A^+B_2. By $n-1$ such steps it appears that A^+B_i $(i=2\cdots n)$ would have no point in common with a and hence A^+A^- would not meet a.

The proof of statement (2) depends on the observation that any point P of α but not of a is such that one and only one of the segments PA^+ and PA^- meets a. Otherwise the triangle PA^+A^- would meet the line a only in the point A or else in points of all three sides.

Corollary 1 (I–VIII). A line that meets the boundary of a simple polygon but does not meet any of its vertices meets the boundary of the polygon in an even number of points.

Corollary 2 (I–IX). Any plane α decomposes a space in which it lies into two regions.

DEF. 11. If A and B are two distinct points, the *half-line* AB consists of the segment AB, B, and the prolongation of AB beyond B. If A, B, C are three non-collinear points, the *half-plane* (AB, C) is the one of the two regions, into which the line AB decomposes the plane ABC, that contains C. The two half-planes determined by a line in any plane are called the two *sides* of the line. If A, B, C are non-collinear, the *boundary of the angle* BAC consists of A and the points of the half-lines AB and AC. The *interior of the angle* consists of all points in any region of the plane that does not include the boundary and does include a point X satisfying the order relation PXQ where P is a point of the half-line AB and Q of the half-line AC.

TH. 27 (I–VIII). Two non-intersecting complanar lines (if such exist) decom-

pose their plane into three regions, two intersecting lines decompose it into four regions, and the boundary of an angle decomposes it into two regions.

Proof. Call the two regions into which a line decomposes a plane + and −; and then apply the method of theorem 26 to the + and − regions separately. (The new regions will be conveniently designated by + +, + −, − +, − −.)

Corollary 1. In the case of an angle one of the two regions specified by theorem 27 is the interior of the angle. The boundary of an angle meets the boundary of any polygon in its plane and having no vertex or multiple point on the boundary of the angle in an even number of points.

Corollary 2. The boundary of a triangle decomposes the plane in which it lies into two regions, one of which is the interior (def. 5). The other region, which contains lines not intersecting the boundary of the triangle, is called the exterior.

TH. 28 (I–VIII). The boundary of a simple polygon lying entirely in a plane α decomposes α into two regions.

Proof. The proof depends upon two lemmas.

Lemma 1. *If a side of a polygon q intersects a side of a polygon p_n in a single point O not a multiple point of p_n or q, then p_n and q, whether simple or not, have at least one other point in common.* If $n=3$ (q having any number of sides, m) the theorem reduces to corollary 2, theorem 27. We assume without loss of generality that no three vertices P_{i-1}, P_i, P_{i+1}, are collinear and prove the lemma for every n by reducing to the case $n=3$. Let p_n have n vertices with the notation such that the side P_1P_2 meets q in the side $Q_1'Q_2'$ where the segment $Q_2'O$ contains no interior point of the triangle $P_1P_2P_3$. By the case $n=3$, q meets the boundary of the triangle $P_1P_2P_3$ in at least one point other than O. If this point is on the broken line $P_1P_2P_3$ the lemma is verified. If not, q has at least one point on P_1P_3, and at least one of the segments $Q_1'Q_2'$, $Q_2'Q_3'$ has no point or end-point on P_1P_3. Let this segment be one segment of a broken line $Q_kQ_{k+1}\cdots Q_{j-1}Q_j$ of segments of q not meeting P_1P_3 but such that $Q_{k-1}Q_k$ and Q_jQ_{j+1} do each have a point or end-point in common with P_1P_3. ($1 \leqq k < j \leqq m$; if $k=1$, $Q_{k-1}=Q_m$; if $j=m$, $Q_{j+1}=Q_1$). If O_j is the point common to P_1P_3 and Q_jQ_{j+1} or Q_{j+1}, and O_k the point common to P_1P_3 and $Q_{k-1}Q_k$ or Q_{k-1}, the broken line $O_kQ_kQ_{k+1}\cdots Q_{j-1}Q_jO_j$, has a point inside and also a point outside the triangle $P_1P_2P_3$ and cuts the broken line $P_1P_2P_3$ only once. Hence it has a point inside and a point outside any triangle of which P_1P_3 is a side. On this account if $P_1P_3P_4$ are not collinear, and obviously, if $P_1P_3P_4$ are collinear, q must meet either P_3P_4 or P_4 or P_4P_1. If q does not meet P_3P_4 or P_4, we proceed with $P_1P_4P_5$ as we did with $P_1P_3P_4$. Continuing this process, we either verify the lemma or come by $n-2$ steps to the triangle $P_1P_{n-1}P_n$ and find that q must intersect the broken line $P_{n-1}P_nP_1$, which also verifies the lemma.

Lemma 2. A point P of the boundary of a polygon p_n lying in a plane α is said to be *accessible* from a point O of α if there exists a broken line joining O to P and not meeting the boundary of the polygon in any point other than P. *Every point of the boundary of a simple polygon p_n is accessible from every point O of α, not on the boundary of p_n.* That there is at least one point of p_n accessible from O is seen by considering any line through O meeting the boundary of p_n but not meeting a vertex of p_n. This line meets p_n in a finite number of points and hence in a point P' of a side P_jP_{j+1} such that the segment OP' contains no point of p_n.

If P' is any point of a side P_iP_{i+1} of p_n accessible from O by means of a broken line $OQ_1Q_2\cdots Q_nP'$, it is evident that P_i is accessible from O by means of a similar broken line. For the lines joining P_i to each of the other vertices of p_n meet Q_nP' in at most a finite number of points. There is, therefore, a point Q' such that the segment $Q'P'$ contains none of these points and thus the segment joining P_i to a point of $Q'P'$ does not meet p_n in other points than P_i.

Considerations similar to those just adduced show that if P'' is any point of a side P_iP_{i+1} such that P_i is accessible from O, P'' is also accessible. Now since P' of P_jP_{j+1} is accessible from O, so is every point of P_jP_{j+1} and also P_{j+1}, and hence every point of $P_{j+1}P_{j+2}$, and so on for the whole polygon.

If p_n is any polygon of α, let A and B be two points such that the segment AB intersects a side P_1P_2 but does not meet any other point of the boundary of p_n. By lemma 1, every broken line joining A to B meets p_n. Hence the boundary of any plane polygon whatever decomposes its plane into at least two regions.

If the boundary of a *simple* polygon p_n should decompose α into three regions, let P be a point of the side P_1P_2. P being accessible from each region, there are three segments belonging to different regions whose mutual end-point is P. Two of these segments PC and PD must lie in the same one of the two half-planes defined by P_1P_2. C' and D' being points of PC and PD such that no line joining two vertices of p_n meets PC' or PD', it is evident that $C'D'$ does not meet p_n and hence C' and D' belong to the same region, contradicting the hypothesis of three regions. The boundary of a simple polygon therefore decomposes a plane in which it lies into two and only two regions.

The proofs of the following theorems of this section are similar to the preceding, and therefore are omitted.

Def. 12. If A, B, C, D are four non-complanar points, the *boundary of the dihedral angle* of the half-planes (AB, C) and (AB, D) consists of the line AB and the half-planes (AB, C) and (AB, D). If AB, AC, AD are three non-complanar half-lines, the *boundary of the trihedral angle* (A, BCD) consists of *the point* A (the *vertex*), the half lines AB,

AC, AD (the *edges*) and the interiors of the angles BAC, CAD. DAB (the *faces*).

TH. 29 (I–IX). Two non-intersecting planes (if such exist) decompose a space in which they lie into three regions, two intersecting planes decompose it into four regions, and a dihedral angle or a trihedral angle decomposes it into two regions.

DEF. 13. The *interior of a dihedral angle* is that region of the two defined by theorem 29 which includes a point X in the order PXQ where P is a point of one of the half-planes of the boundary and Q a point of the other. The *interior of a trihedral angle* (A, BCD) is that of the two regions defined by theorem 29 which includes a point X in the order PXQ where P is a point of the edge AB and Q of the side CAD. The *exterior* of a dihedral or trihedral angle is that one of the two regions defined by theorem 29 which is not interior.

TH. 30 (I–IX). A plane through the vertex and an interior point of a trihedral angle meets the boundary in two half-lines of which one may be an edge and the other interior to a side or each may be interior to a side different from the side to which the other is interior.

DEF. 14. Let a finite or infinite set of complanar lines $\cdots a \cdots b \cdots c \cdots d \cdots k \cdots$ pass through a point O. Let M and N be two points of any line a in the order MON. Let C be any point of a line c. If the lines $\cdots b \cdots$ meet MC in a set of points $\cdots B \cdots$ in the order $M \cdots B \cdots C$ and the lines $\cdots d \cdots k \cdots$ meet CN in a set of points $\cdots D \cdots K \cdots$ in the order $C \cdots D \cdots K \cdots N$, then the set of lines is in the order $a \cdots b \cdots c \cdots k \cdots$. In the special case of the order $abcd$, a and c are said to separate b and d.

TH. 31 (I–VIII). The above definition is independent of the triangle MNP. The notation can be permuted cyclically or reversed. From $a \cdots b \cdots c \cdots k$ and $abkl$, follows $a \cdots b \cdots c \cdots kl$. If a and c separate b and d, a and b do not separate c and d nor do a and d separate b and c. From $abcd$ and $abce$ $(d \neq e)$ follows either $abcde$ or $abced$. In case of the order $abcd$, any segment joining a point of a to a point of c meets one or other of the lines b and d. Any segment joining a point of a to a point of b either meets both c and d or neither.

DEF. 15. Let a finite or infinite set of planes $\alpha \cdots \beta \cdots \gamma \cdots \lambda$ pass through a line o. Intersect o by a plane π. Then if a is the intersection of α and π, b of β and π, etc., and the lines $a \cdots b$, etc., are in the order $a \cdots b \cdots c \cdots l \cdots$, the planes are in the order $\alpha \cdots \beta \cdots \gamma \cdots \lambda \cdots$.

TH. 32 (I–IX). The above definition is independent of the plane π and analogous statements to those of theorem 30 hold for the planes α, β, etc.

§ 5. *Continuity.*

AXIOM XI. *If there exists an infinitude of points, there exist a certain pair of points AC such that if $[\sigma]$ is any infinite set of segments of the line AC, having the property that each point which is A, C, or a point of the segment AC is a point of a segment σ, then there is a finite sub-set $\sigma_1, \sigma_2, \cdots, \sigma_n$ with the same property.*

TH. 33 (I–VIII, XI). If PQ is any segment and $[\sigma]$ any infinite set of segments of the line PQ, having the property that each point which is P, Q, or a point of the segment PQ is an interior point of a segment σ, then there is a finite subset $\sigma_1, \sigma_2, \cdots, \sigma_n$ having the same property.

Proof. In case of the order $APQC$ consider $A'P$ and QC' (where A' and C' are in the order $A'ACC'$) as segments of $[\sigma]$ and the theorem is a corollary of XI.

In case PQ is not on the line AC but $P = A$, let O be a point in the order OCQ. If $[R]$ is the set of those end points of segments σ that lie between P and Q, by § 3 each of the lines OR meets AC in a point B. Thus every segment σ which lies between P and Q corresponds to a segment σ' between A and C. To any segment σ whose end points $S_1 S_2$ are in the order PS_1QS_2 let correspond $D_1 D_2 = \sigma'$ where D_1 is the point of intersection of OS_1 with AC and D_2 any point in the order ACD_2. Similarly in the case QS_1PS_2.

By XI there is a finite subset of $[\sigma']$, $\sigma_1', \sigma_2', \cdots, \sigma_n'$ of which A, C, and every point of AC are interior points. Any set of σ's corresponding to $\sigma_1', \cdots, \sigma_n'$ is the required set $\sigma_1, \cdots, \sigma_n$.

If $P = A$ and Q is any point of the line AC let Q' be any point not on the line AC. The theorem holds for PQ' by the preceding paragraph and hence by a similar argument for PQ. If $P \neq Q$ and PQ is any segment not of the line AC, the theorem follows by the intermediation of the segment AP.

TH. 34 (I–VIII, XI). If a segment AB consists of two sets of points $[P]$ and $[Q]$ such that no point P is between two points Q and no point Q between two points P then there exists one and only one point O in the order POQ for every pair of points P and Q ($P \neq O$, $Q \neq O$).

Proof. Supposing the conclusion of the theorem not valid assign the notation so that there is the order $APQB$; then including A there is a segment not including any point Q and including B there is a segment not including any point P; including every point P there is a segment including no point Q and including every point Q a segment including no point P. Of this set of segments $[\sigma]$ there is (33) a finite sub-set including A, B, and every point of AB. Assign notation to those end points of segments of this set which include points P so that there is the order $A_1 A_2 \cdots A_m AP_1 P_2 \cdots P_n$; and to those end points of segments of this set which include points Q so that there is the order $Q_k \cdots Q_2 Q_1 BB_l \cdots B_1$.

By hypothesis we have

$$A_1 A_2 \cdots A_m A P_1 P_2 \cdots P_n Q_k Q_{k-1} \cdots Q_2 Q_1 B B_1 \cdots B_l .$$

One of the set of segments whose $n + m + k + l$ end points are here enumerated must include points between P_n and Q_k but such a segment includes both points of P and of Q, contrary to the hypothesis about $[\sigma]$.

That there is only one point O is shown by remarking that if there were two points, O and O', in the order $POO'Q$ for every P, Q there would (6) be a point S in the order OSO' and hence in the orders PSO' and OSQ. But S must be either a P or a Q. In the first case the hypothesis would be contradicted by OSQ and in the second case by PSO'.

DEF. 16. A point P is a *limit point* of a set of points $[S]$ of a line AB if every segment of AB which contains P contains some point of $[S]$ distinct from P.

The following two theorems can be proved either directly from theorem 33 or in the well-known way from theorem 34.

TH. 35 (I–VIII, XI). Every infinite set of points lying on a segment has at least one limit point.

TH. 36 (I–VIII, XI). If A and C are any two points and a set of points $[B]$ is in the order ABC there is a point P in the order ABP for every $B \neq P$, and such that if Q is any point in the order ABQ for every B, either $P = Q$ or APQ.

TH. 37 (I–VIII, XI). If all the lines through a point C, in a plane α, consist of two sets $[s]$ and $[t]$ such that each set contains at least two lines, and no two lines of one set separate any two lines of the other set, then there are two lines o_1 and o_2 that separate every s $(\neq o_1, \neq o_2)$ from every t $(\neq o_1, \neq o_2)$.

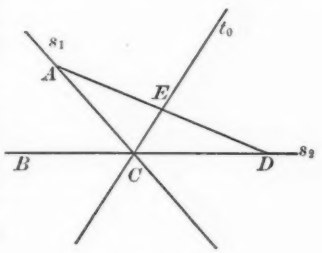

FIG. 20.

Proof. Let s_1 and s_2 be two lines of $[s]$, and A any point of s_1, while B and D are points of s_2 in the order BCD. By § 4, supposing that some t intersects AD there is no t that intersects AB. Let E be the point of intersection of some line t_0 with AD. The theorem follows at once as a corollary of theorem 34, by considering the two sets of points of intersection of $[s]$ and $[t]$ with the segments AE and ED respectively.

§ 6. *Parallel lines.*

TH. 38 (I–VIII, XI). If a is any line of a plane α, through any point C of α there is at least one line of α that does not intersect a.

TH. 39 (I–VIII, XI). If there is more than one such line, there are two lines, c_1 and c_2, through C, not meeting a that separate the lines that do not intersect a from those that do intersect a.

Proof of 38.* Let Q and R be any two points of a, and let $[s]$ be the set of all lines through C that meet a in points S in the order QRS. Let $[t]$ be the set of all other lines through C. No two lines s separate two lines t; for in that case one of the lines t would intersect a on the prolongation of QR beyond R. Hence (37) there are two lines b_1 and b_2 that separate every line s from every line t. Not both of these lines meet a. For if this were so, call their points of intersection B_1 and B_2 and the points of intersection of an s line, S, and of a t line, T. If there is a point T in the order B_1TB_2, there are points S' and S'' in the order $S'B_1B_2S''$, and hence a T point between two S points,—a contradiction with the hypothesis that all points of the prolongation of QR are S points. If there is a point S in the order B_1SB_2, there are points T' and T'' in the order $T'B_1B_2T''$ and hence in the order $T'ST''$ and therefore a T point on the prolongation of QR beyond R.

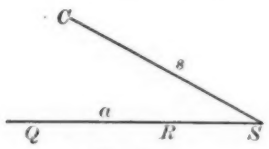

FIG. 21.

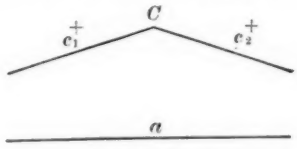

FIG. 22.

Proof of 39. Let all the lines through C that meet a be $[s]$ and all that do not $[t]$. Then the existence of c_1 and c_2 follows at once from theorem 37. c_1 or c_1 cannot intersect a; for in that case we should have $S_1C_1S_2$ or $S_1C_2S_2$.

DEF. 17. In case there are two lines c and c_1 the line a lies wholly in one of the four regions into which the plane is decomposed by c_1 and c_2. Call the two half-lines, c_1^+ and c_2^+, that bound this region of the plane the *half-lines parallel to* a. a and the two parallel half-lines c_1^+ and c_2^+ separate from the rest of the plane a region of the plane which lies *between* them and consists of all points that can be joined by a segment not meeting a or c_1^+ or c_2^+ to a point B in the order CBQ. In case the lines c_1 and c_2 coincide in a line c, that line is called *the parallel to* a.

TH. 40 (I–IX). If a has two parallel half-lines, any line through a point between a and its parallel half-lines, c_1^+ and c_2^+, meets either a or c_1^+ or c_2^+.

Proof. Let O be a point not in the plane α. The planes Oc_1 and Oc_2 and Oa meet in three lines, OC, a_1, and a_2. Let the line through a point between a and c_1^+ and c_2^+ be b. Then, the plane Ob, passing through the interior of the trihedral angle whose vertex is O, meets two of the sides o" one side and one edge.

* That XI is essential for this theorem is proved by K_{XI}, § 4, chap. I.

Hence there is at least one line o' common to the plane Ob and a side of the trihedral angle, and by the lemma below, o' meets a or c_1^+ or c_2^+.

Lemma. If o' is any line through O in the face Oa of the trihedral angle, o' meets a; for the plane Co' meets α in a line a that passes through a point in the interior of the angle between c_1^+ and c_2^+. If o'' is any line through O in the face Oc_1^+, it meets c_1^+; for joining o'' to a point C' of the half-line of c_2 other than c_2^+, this plane meets Oa in a line o' that must intersect a in a point A. As the points A and C are on opposite sides of c_1^+, the plane $o''C'$ meets c_1^+, and therefore o'' meets c_1^+.

Th. 41 (I–IX). If in a plane α through a point C there is only one line c parallel to a, any line of α that meets one of the lines a and c meets the other.

Proof. It follows as in the lemma to theorem 40 that if O is a point outside α, and o the intersection of Oc and Oa, any line of one of these planes that passes through O and is distinct from o meets a if it is in Oa and c if it is in Oc.

If a' is a line through a point A of a the plane Oa' meets Oc in a line o' distinct from o, and o' meets c by the first paragraph. Similarly, if c' is a line through a point C' of c, the plane Oc' meets Oa in a line o' distinct from o, and hence o' meets a.

Th. 42 (I–IX, XI). If a is a line of a plane α and through one point C, not on a, there is only one line c that does not intersect a, then through any point C' of α not on a there is only one parallel to a.

Proof. Suppose that through a point C not between a and c there are two parallels c_1 and c_2 to a. These lines are also parallel to c: for by theorem 41 every line through C that meets c also meets a, and every line that meets a meets c. Then either c lies between a and c_1^+ and c_2^+, or a lies between c_1^+ and c_2^+ and c. Either case is in contradiction with theorem 40. Hence there can be only one parallel through C. The theorem now follows for any point $\overline{C}$ between a and c by considering with a a parallel, on the opposite side of a from $\overline{C}$.

Axiom XII. *If a is any line of any plane α there is some point C of α through which there is not more than one line of the plane α which does not intersect a.*

Th. 43 (I–IX, XI, XII). In any plane α through any point A there is one and only one line parallel to a given line a.

Proof. By XII and theorems 38 and 42.

CHAPTER III.

Projective Geometry.

§ 1. *Preliminary theorems.*

The development of projective geometry from the foundation established in the preceding chapter §§ 1–6, follows methods that are fairly well known.

On this account and for lack of space the proofs of most of the theorems will be omitted. While it will not often be possible to give a reference which furnishes complete details of a demonstration, the citation will generally cover the methods.

Projective geometry is independent of the parallel axiom and so in this chapter no use will be made of § 6, chapter II before § 7 where the euclidean metrical geometry is defined. In the present § 1 are stated some preliminary theorems from which are derived, in the following § 2, definitions of the projective elements analogous to those originally proposed by KLEIN.* In neither of these sections is any use made of the continuity axiom XI.

Lemma. Let π and ρ be two planes intersecting in a line a, and let l and m be two lines of ρ lying on the same side of a. Then if l is complanar with each of two lines b and c of π, and m is complanar with b, it follows that m is complanar also with c.

TH. 44 (I–X). If three lines, a, b, and c, of a plane π, are each complanar with a line l not of the plane π, and a and b are each complanar with another line m, then c is also complanar with m.

TH. 45 (I–X). If a and b are two lines in a plane π, and l and m two lines not in π but each complanar with a and b, then l and m are complanar.

DEF. 18. Two lines a and b lying in the same plane π, define a system of lines consisting of every line of intersection of a plane through a with a plane through b as well as all the lines in π that are complanar with one of the lines of the system that does not lie in π. Such a system of lines is called a *bundle*. The system of all lines in a plane π complanar with a line l not in π is called a *pencil*.

TH. 46 (I–X). Every two lines of a bundle are complanar and define the same bundle. Through any point of space passes one line of a given bundle. Any two points B and C not in the same line of a bundle A define with A a plane including all lines of A passing through points of the line BC. Two distinct bundles have in common at most one line.

DEF. 19. If A and B are two bundles, through every point O of space there passes one line of each bundle. If these lines do not coincide they define a plane. The system of planes thus defined by two bundles is called a *pencil of planes*. Every line of A or B not common to A and B lies in one and only one plane of the pencil. A bundle every one of whose lines lies in a plane of the pencil is said to be *incident with* the pencil.

A special case of a pencil of planes is the set all of planes through a line.

TH. 47 (I–X). If $A_1B_1C_1$ and $A_2B_2C_2$ are two triangles of a plane π, such

* F. KLEIN, Mathematische Annalen, vol. 6 (1873), p. 112. Further details are given by M. PASCH, l. c., pages 40 to 72, and by F. SCHUR, *Ueber die Einführung der sogenannten idealen Elemente in die projective Geometrie*, Mathematische Annalen, vol. 39 (1891), p. 113. A very elegant exposition is due to R. BONOLA, *Sulla introduzione degli enti improprii in geometria projettiva*, Giornale di Matematiche, vol. 38 (1900), p. 105.

that the three bundles defined by the three pairs of sides A_1B_1 and A_2B_2, B_1C_1 and B_2C_2, C_1A_1 and C_2A_2, each has a line in a certain plane σ, $(\sigma \neq \pi)$ then the joints of corresponding vertices, A_1A_2, B_1B_2, C_1C_2, lie in the same pencil.

TH. 48 (I–X.) If a pencil of planes defined by two bundles L_1 and L_2 meets a plane π in three lines, a, b, and c, these three lines lie in the same pencil of lines.

Corollary 1. Any bundle having a line in each of two planes of a pencil is incident with the pencil.

Corollary 2. Any two bundles incident with a pencil of planes determine that pencil.

TH. 49 (I–X). If ABC and $A_1B_1C_1$ are two triangles of a plane π such that the lines AA_1, BB_1, CC_1, are in the same pencil, then the bundles defined by pairs AB, A_1B_1, BC, B_1C_1, and AC, A_1C_1, lie in the same pencil of planes.

Corollary. If two triangles ABC and $A'B'C'$ are so situated in a plane that the lines joining their corresponding vertices AA', BB', CC', meet in a point P, and the corresponding sides AB, $A'B'$, etc., meet in three points, C_1, C_2, C_3 then C_1, C_2, C_3 are collinear; and conversely.

TH. 50 (I–X). If three bundles, A, E, and C lie in one pencil of planes, whereas three bundles B, C, and D lie in another pencil of planes, then there is a bundle F incident at once with the pencils AB and DE.

§ 2. *The projective elements.*

DEF. 20. A *projective point* is a bundle of lines.

DEF. 21. A *projective line* is a pencil of planes. Three points incident with the same line are collinear.

DEF. 22. A *projective plane* is the set of all projective points collinear with the projective point O and any point of a projective line o not incident with O (including O and the points incident with o). Any point of the plane is said to be *incident with* the plane.

DEF. 23. A projective point is called *proper* if the bundle of lines defining it meet in a point. A projective line or plane is proper if there is incident with it a proper point; otherwise it is *improper* or *ideal*.

It will immediately become evident that a proper projective point has the same incidence relations as a point in the sense of chapter II. For the rest of this chapter we shall mean by "point" a projective point, and by "proper point" a proper projective point.

By corollary 2, theorem 48, any two points incident with a line determine that line. Let a plane π be determined by a line a and point B not incident with a. That any other point and line incident with π determine it, is an immediate

deduction from theorem 38. This amounts to saying that any three points incident with π determine it, and that any line, two of whose points are incident with π is also incident with π. It follows that any two lines incident with π are incident with one, and only one, common point.

A line incident with a proper point is by def. 23 and by theorem 25 incident with another proper point, and hence the ordinary line defined by these points is contained in the projective line. Consequently, every plane incident with a with a proper point is incident with three non-collinear proper points, and therefore the ordinary (chapter II) plane determined by these three points is included in the projective plane.

By def. 21, every two proper planes are incident with one, and only one line, proper or improper. A proper plane λ and an improper μ are incident with one and only one improper line. For let m be any line of μ; it is by definition the intersection of two proper planes α and β through two proper points A and B of λ that are therefore incident with two proper lines a and b of λ. a and b define a point at once incident with m and λ. Hence every line m of μ is incident with a point L of λ. But as three non-collinear points determine a plane, these points L must be incident with a line, which proves our proposition.

Finally, two improper planes, ρ and σ, are incident with one and only one line. For a proper plane α is incident with one line of each of them, so that the point incident with each of these lines is incident with each of the planes ρ and σ. Another proper plane β gives another point, and just as in the preceding paragraph, these two points determine the one and only one line incident with ρ and σ.

As obvious results of the above argument, we have:*

TH. 51 (I–X). Two points are incident with one and only one line.

Two planes are incident with one and only one line.

TH. 52 (I–X). Three points not incident with the same line are incident with one and only one plane.

Three planes not incident with the same line are incident with one and only one point.

TH. 53 (I–X). A line and a point not incident with it are incident with one and only one plane.

A line and a plane not incident with it are incident with one and only one point.

TH. 54 (I–X). Two lines incident with the same plane are incident with one and only one point.

* No attempt is here made to obtain an *independent* system of basal theorems for projective geometry. The foundations of projective geometry as a science by itself have been studied by M. PIERI, *Sui principii che reggono la geometria della retta*, Atti della Reale Accademia della Scienze di Torino, vol. 36 (1901), p. 335. *I principii della geometria di posizione* ···, Memorie della Reale Accademia della Scienze di Torino, vol. 48 (1899), p. 1.

Two lines incident with the same point are incident with one and only one plane.

TH. 55 (I–X). If two points are incident with a plane, any line incident with each of them is incident with the plane.

If two planes are incident with a point, any line incident with each of them is incident with the point.

The terms pencil and bundle, which were used of the elements of chapter I, will now be applied in an analogous way to the projective elements.

DEF. 24. The set of all lines incident at once with any plane α and any point A (incident with α) is called a *pencil* of lines.

The set of all points incident with a line a is called a *pencil* of points.

The set of all planes incident with a line a is called a *pencil* of planes or *axial pencil.*

Pencils of lines, points, and planes are called *one-dimensional forms* or *forms of the first grade.*

DEF. 25. A *two-dimensional form* or *form of the second grade* is one of the following:

1. The set of all lines incident with a point.
2. The set of all lines incident with a plane.
3. The set of all planes incident with a point.
4. The set of all points incident with a plane.

1 and 3 are also called *bundles of lines* and *bundles of planes.* The system of all points and lines incident with a plane is called a *plane system* or *field;* and the set of all planes and lines incident with a point is called a *point system* or *point field.*

DEF. 26. The set of all points in space and the set of all planes in space are called *three dimensional forms* or *forms of the third grade.* The set of all points and planes in space is the space system or space field.

DEF. 27. A *figure* is any set of points, lines, and planes.

DEF. 28. If A is a point incident with no point of a figure w (consisting of points and lines) the system of all elements at once incident with A and the elements of w is the *projection* of w from A. A is called a *center of perspectivity.* If w' is a figure consisting of lines and planes, and a (or α) a line (or plane) not incident with any element of w', then the system of all elements at once incident with a (or α) and w' is the *section* of w' by a (or α). If two figures have a projection or section in common, or if one is a section of the other, they are said to be *perspective* figures.

DEF. 29. If $1, 2, 3, \cdots$ are elements of a one-dimensional form, and $1', 2', 3', \cdots$ are elements of another one-dimensional form, perspective with $1, 2, 3, \cdots$, we write $(1, 2, 3, \cdots) \barwedge (1', 2', 3', \cdots)$. If

$$(1, 2, 3, \cdots) \barwedge (1', 2', 3', \cdots) \cdot \cdot \barwedge (1^n, 2^n, 3^n, \cdots) \quad (n = 2, 3, \cdots),$$

we say that the figures $(1, 2, 3, 4, \cdots)$ and $(1^n, 2^n, 3^n, 4^n, \cdots)$ are *projective*, and use the notation $(1, 2, 3, 4, \cdots) \pi (1^n, 2^n, 3^n, 4^n, \cdots)$.

§ 3. *Order and continuity of projective elements.*

DEF. 30. A finite or infinite set of collinear points are in the *order* $A \cdots B \cdots C \cdots K$ if they are projected from a proper point O by lines in the order $a \cdots b \cdots c \cdots k$ (see chapter I, § 4).

Lemma *a*. This definition is independent of the choice of O.

Lemma *b*. If two sets of points $A, B, C, \cdots$ and $A'B'C' \cdots$ are sections of the same (one-dimensional) pencil of lines in such a way that A, A', B, B', etc., are incident with the same line of the pencil, then if one set is in the order $A \cdots B \cdots C \cdots K$, the other set is in the order $A' \cdots B' \cdots C' \cdots K'$.

Lemma *c*. If two ranges l_1 and l_2 are sections of a pencil of planes S and the points A_1 and A_2, B_1 and B_2, etc., are incident with the same plane, then if the order of a set of points on l_1 is $A_1 \cdots B_1 \cdots C_1 \cdots K_1$, the order of the corresponding set on l_2 is $A_2 \cdots B_2 \cdots C_2 \cdots K_2$.

DEF. 31. A set of elements of any form of the first grade (not a pencil of points) are in the order $\cdots l \cdots m \cdots n \cdots k \cdots$ if their section by a line is a set of points in the order $\cdots L \cdots M \cdots N \cdots K \cdots$. If four elements are in the order 1 2 3 4, 1 and 3 are said to *separate* 2 and 4.

TH. 56 (I–X). If 1 2 3 are any three distinct elements of a one-dimensional form, there exists an element 4 in the order 1 2 3 4. If elements 1, 2, 3, 4 are in the order 1 2 3 4 they are distinct. The notation for the order of a set of elements $\cdots l \cdots n \cdots m \cdots k \cdots$ of a one-dimensional form can be permuted cyclically or reversed. No other permutation is possible. From $l \cdots n \cdots m \cdots k$ and $l n k p$ follows $l \cdots n \cdots m \cdots k p$. From 1 2 3 4 and 1 2 3 5 $(4 \neq 5)$ follows either 1 2 4 5 or 1 2 5 4. Any set of elements $\cdots l' \cdots k' \cdots$ perspective or projective with a set in the order $\cdots l \cdots n \cdots m \cdots k \cdots$ in such a way that l' corresponds to l, etc., are in the order $\cdots l' \cdots n' \cdots m' \cdots k' \cdots$.

TH. 57 (I–XI). If all the elements of a one-dimensional form consist of two sets, such that each set consists of at least two elements, and no two elements of one set separate two elements of the other set, then there exist two elements p and p' that separate each element (distinct from p and p') of one set from each element (distinct from p and p') of the other set.

§ 4. *Principle of duality.*

All the theorems of projective geometry can be deduced from theorems 51–57. These theorems remain entirely unchanged if the words point and plane are interchanged. Hence anything that can be deduced from them about points

can be deduced also about planes. Hence we have, referring to a proposition deducible from theorems 51–57 as a projective proposition:

TH. 58 (I–XI). *Fundamental theorem of duality.* Any valid projective proposition remains valid if the words point and plane are interchanged in its complete statement.

From this duality of space follows a like duality among the planes and lines or points and lines of any point- or plane-field. If π is any plane, any theorem about the incidence and order of the lines and points in π will hold for the incidence and order of the planes and lines obtained by projecting the lines and points of π from a point O. The space dual of this latter theorem is a theorem about points and lines, in any plane σ; or in particular about the plane $\sigma = \pi$. Hence we have:

TH. 59 (I–XI). Any valid projective proposition about points and lines incident with a plane π remains valid if the words *point* and *line* are interchanged.

As the space dual of theorem 59 we have:

TH. 60 (I–XI). Any valid projective proposition about lines and planes incident with a point P remains valid if the words *plane* and *line* are interchanged.

The general term incidence has been used in this section to bring out the duality of space in a formal way. In the following sections, however, we shall use the words intersect, lie in, are on, etc., according to the ordinary usage.

§ 5. *Harmonic conjugates.*

The following theorems are well-known and are satisfactorily proved in the standard text-books.

TH. 61 (I–X). If A, B, C are three points of a line l, and A', B', C' are any three points of any other line l', ABC can be projected to $A'B'C'$ by the use of two centers of perspectivity.

Corollary. If A, B, C, and A', B', C' are on the same line l, three centers of perspectivity are sufficient.

TH. 62 (I–X). If A, B, C, D are any four points of a line,

$$(ABCD) \overline{\wedge} (BADC) \overline{\wedge} (CDAB).$$

DEF. 32. The figure consisting of three non-collinear points and the three lines incident with them by pairs is called a *triangle.*

DEF. 33. The figure consisting of four complanar points (no three of which are collinear) and the six lines incident with them by pairs is called a *complete quadrangle.* The four points are called the *vertices;* the six lines, the *sides;* two sides that do not have a vertex in common are *opposite sides;* and the points of intersection of opposite sides are *diagonal points.* The triangle of the diagonal points is called the *diagonal triangle.*

DEF. 34. The plane dual of the above figure is a *complete quadrilateral.* It has four sides, six vertices, and three diagonal lines, etc.

TH. 63 (I–X). Let ABC and $A'B'C'$ be two triangles lying in the same or in different planes. If the joins of corresponding vertices, AA', BB', CC', meet in a point, the corresponding sides, AB with $A'B'$, BC with $B'C'$, AC with $A'C'$, intersect in three points of a line. Conversely, if the intersections of corresponding sides lie on a line the joins of corresponding vertices meet in a point.

TH. 64 (I–X). If five sides of one complete quadrangle intersect five sides of another complete quadrangle (no point of intersection being a vertex) in collinear points, then the point of intersection of the sixth side of one with the sixth side of the other lies on the same line with the other five intersection points.

DEF. 35. If A and C are diagonal points of a quadrangle, and B and D the intersections of the remaining pair of opposite sides with the line AC, D is called the fourth harmonic or harmonic conjugate of B with respect to A and C.

TH. 65 (I–X). If D is the harmonic conjugate of B with respect to A and C, there is only one such point D, B is the harmonic conjugate of D with respect to A and C, and the points A, C are separated by B, D.

DEF. 36. If D is the fourth harmonic of B with respect to A and C, the pair BD are said to separate AC harmonically; $ABCD$ are sometimes said to be four harmonic points.

TH. 66 (I–X). If $(ABCD) \barwedge (A'B'C'D')$ and the pair BD separates the pair AC harmonically, then $B'D'$ separates $A'C'$ harmonically. *Conversely*, if B and D separate A and C harmonically, and A', B', C', D' are any four points such that B', D' separate A', C' harmonically, then $(ABCD) \barwedge (A'B'C'D')$. If B and D separate A and C harmonically, then A and C separate B and D harmonically.

Corollary. If $ABCD$ are four harmonic points, besides the perspectivities of theorem 62 $(ABCD) \barwedge (ADCB) \barwedge (CBAD)$.

§ 6. *The fundamental theorem of projective geometry.*

DEF. 37. If A, B, C are any three points of a line, a point D is said to be harmonically related to A, B, C if it is any one of a finite set of points $D_1 \cdots D_n$ $(n \geqq 1)$ such that D_1 is the fourth harmonic of one of A, B, C with respect to the other two and D_k $(k = 2 \cdots n)$ the fourth harmonic of one of the set $ABCD_1 \cdots D_{k-1}$ with respect to two others of the set.

TH. 67 (I–XI). If A, B, C are any three points of a line and P and Q any two other points of the same line then there are two points D and E which at the same time are harmonically related to A, B, C and separate P and Q.*

* F. KLEIN (Mathematische Annalen, vol. 6 (1873) p. 139) first pointed out that VON STAUDT's proof of the fundamental theorem was incomplete without the use of some such axiom as XI.

TH. 68 (I–XI). *The fundamental theorem.* If $ABCD$ are four collinear points and $(ABCD) \overline{\wedge} (A'B'C'D')$ then by any process of projection and section for which $(ABCD) \overline{\wedge} (A'B'C'D'')$, $D' = D''$.*

TH. 69 (I–XI) If A, B and C, D are two pairs of points that do not separate one another then there exists one and only one pair P, Q that at once harmonically separates A, B and C, D.

By means of this theorem it is seen that any one to one correspondence preserving harmonic relations also preserves order and then by theorem 67 and the principle of duality we obtain the following general form of the "fundamental theorem."

DEF. 38. A one-to-one correspondence between two forms (or of a form with itself) is called projective if, whenever elements $1, 2, 3, \cdots$ of the same one-dimensional form correspond to elements $1', 2', 3', \cdots$,

$$(123\cdots) \overline{\wedge} (1'2'3'\cdots).$$

TH. 70 (I–XI). *A more general fundamental theorem.* Any one-to-one correspondence between two one-dimensional forms by which every four harmonic elements of one form correspond to four harmonic elements of the other form, is projective.

TH. 71 (I–XI). A one-to-one correspondence between two forms I and I′ (where I may be the same as I′) of the same grade higher than the first is projective if every one-dimensional form of elements of I corresponds to a to a one-dimensional form of I′, and reciprocally.

DEF. 39. A projective correspondence by which points correspond to points is a *collineation.* A projective correspondence by which elements of one kind correspond to elements of another kind is called *polar.*

§ 7. *Involution and polar system.*

DEF. 40. An *involution* is such a projective correspondence of a one-dimensional form with itself that if an element 1 corresponds to 1′ then 1′ corresponds to 1. Pairs of elements such as 1 and 1′ are called pairs of *conjugate* elements. The following theorems stated for pencils of points apply by duality to involutions in general.

TH. 72 (I–XI). An involution has either two or no self-corresponding points.

M. PASCH (Vorlesungen über Neuere Geometrie, § 15, Leipzig, 1882) gave a proof which made use of congruence axioms and the so-called Archimedean axiom.

H. WIENER (*Ueber die Grundlagen und den Aufbau der Geometrie,* Jahresbericht der Deutschen Mathematikervereinigung, vol. 1, p. 47, vol. 3, p. 70) and SCHUR (Mathematische Annalen, vol. 51 (1898), p. 401, vol. 55 (1902), p. 265) have shown that it can be demonstrated by congruence axioms alone without the Archimedean axiom.

L. BALSER (Mathematische Annalen, vol. 55 (1902), p. 293) has given a proof based upon hypotheses equivalent to ours.

Corollary. If an involution has two fixed points, A, B, they separate harmonically every pair of corresponding points.

TH. 73 (I–XI). If A, A', B, B' are arbitrary points of a line, there exists one and only one involution in which A and A', B and B' are conjugate points.

Corollary. The theorem is true also if $A = A'$ or $B = B'$, or both.

TH. 74 (I–XI). The three pairs of opposite sides of a complete quadrangle $QRST$ are cut in three pairs of an involution by any straight line which lies in the plane of the quadrangle and passes through none of its vertices.

TH. 75 (I–XI). If two pairs, AA', BB', of an involution do not separate each other, no two pairs of the involution separate each other, and the involution has two fixed points. If two pairs, AA', BB', separate each other, every two pairs of the involution separate each other, and the involution has no fixed point.

DEF. 41. An involution with two fixed points is called *hyperbolic*. An involution with no fixed point is called *elliptic*.

TH. 76 (I–XI). If B and C are two points of a line, there is one, and only one, pair of a given elliptic involution that separates B and C harmonically.

TH. 77 (I–XI). If two pencils are projective, an involution in one corresponds to an involution in the other.

DEF. 42. The points and lines of a plane constitute a *polar system* if they are in such a reciprocal one to one correspondence that to the $\frac{\text{point}}{\text{line}}$ incident with any two $\frac{\text{lines}}{\text{points}}$ corresponds the $\frac{\text{line}}{\text{point}}$ incident with the corresponding pair of $\frac{\text{points}}{\text{lines}}$. A point is the *pole* of its corresponding line, and a line the *polar* of its corresponding point. A polar system is *elliptic* if no element is incident with its corresponding element; it is *hyperbolic* if some element is incident with its corresponding element. A $\frac{\text{line } l'}{\text{point } L'}$ is *conjugate* to a $\frac{\text{line } l}{\text{point } L}$ if it passes through the $\frac{\text{pole}}{\text{polar}}$ of $\frac{l}{L}$.

The proofs of the existence of the various collineation and polar systems depend on constructions that are well-known and for which it is easily verified that our hypotheses are sufficient. See

J. STEINER: *Synthetische Geometrie, Die Theorie der Kegelschnitte*, Leipzig, 1887.

H. SCHROETER: *Theorie der Oberflächen Zweiter Ordnung*, Leipzig, 1880.

K. G. C. VON STAUDT: *Beiträge zur Geometrie der Lage*, Nürnberg, 1856.

In particular, in STEINER'S *Synthetische Geometrie* on pp. 411–414 and 422–424 will be found the proof of the existence of elliptic polar systems.

In the following section we outline the definition and deduction of metric euclidean geometry. For that argument we employ the following theorems:

TH. 78 (I–XI). In any polar system, if a $\frac{\text{line } l}{\text{point } L}$ is conjugate to a $\frac{\text{line } l''}{\text{point } L'}$, $\frac{l'}{L'}$ is conjugate to $\frac{l}{L}$. The system of all such pairs of conjugate $\frac{\text{lines}}{\text{points}}$ of a given $\frac{\text{point}}{\text{line}}$ form an involution. There exist polar systems in which all these involutions are elliptic. A polar system is fully determined by the involutions upon a pair of conjugate $\frac{\text{points}}{\text{lines}}$.

TH. 79 (I–XI). If $A_1A_2A_3$ are the vertices of a triangle and $P_1P_2P_3$ the points of intersection of the lines A_2A_3, A_3A_1, A_1A_2 respectively with a line p, and $M_1M_2M_3$ the harmonic conjugates of $P_1P_2P_3$ with respect to A_2A_3, A_3A_1, A_1A_2 then the three lines joining $M_1M_2M_3$ to the three conjugate points of $P_1P_2P_3$ in any involution on p, meet in a point.

The metric special case of this theorem is that the perpendiculars at the middle points of the sides of a triangle meet in a point. For its proof one has only to consider the complete quadrangle $PM_1M_2M_3$ where P is the intersection of $P_1'M_1$ with $P_2'M_2$, P_1' and P_2' being the conjugate points of P_1 and P_2. It leads at once to the following

TH. 80 (I–XI). Let Σ be an elliptic polar system and $A_1A_2A_3$ any triangle and M_1P_1, M_2P_2 the unique pairs of conjugate points that separate A_2A_3 and A_3A_1 harmonically. If P_3 is the point of intersection of P_1P_2 (or of M_1M_2) with A_1A_2 then the fourth harmonic M_3 of P_3 with respect to A_1A_2 is also its conjugate with respect to Σ. Furthermore the three conjugate lines of the sides of the triangle at M_1, M_2, M_3 meet in a point P, the pole of P_1P_2.

§ 7. *Similar figures.**

DEF. 43. In this section the term *projective transformation* will be used as synonymous with *collineation.* If a point X corresponds to a point X' in a collineation, X is said to be projectively *transformed into* or to *go into*, X'. A *reflection* of the points of a line by a pair of points of the line AA' is a projective transformation by which each point of the line goes into its fourth harmonic with respect to A and A'; i. e., the pairs of corresponding points form an hyperbolic involution; For this transformation we use the notation (AA').

A *reflection* of the points of a $\frac{\text{plane}}{\text{space}}$ by the (non-incident) point A and $\frac{\text{line } a}{\text{plane } \alpha}$ of the $\frac{\text{plane}}{\text{space}}$ is a projective transformation such that each point X of the $\frac{\text{plane}}{\text{space}}$ goes into its fourth harmonic with respect to A and the intersection of AX with $\frac{a}{\alpha}$. We use the notation $\binom{A\alpha}{A\alpha}$.

If by one projective transformation, μ, points A, B, C, D, $\cdots$ go into $A'B'C'D'\cdots$ and by another, ν, $A'B'C'D'\cdots$ go into $A''B''C''D''\cdots$, then the correspondence of $ABCD\cdots$ with $A''B''C''D''\cdots$ is evidently projective; it is called the *product* of ν and μ and written $\nu\mu$. We write $\mu A = A'$ and thus

*For references see footnote, ††, § 1, chap. I.

have $\nu(\mu A) = \nu A' = A'' = (\nu\mu)A$. Further $\rho(\nu\mu) = (\rho\nu)\mu$ and if σ is any reflection σ^2 is the identity. We denote the identity by ω — thus $\sigma^2 = \omega$.

If a transformation is such that every pair of conjugate elements of an involution or polar system, Σ, goes into the same or another conjugate pair, the transformation is said to *leave* Σ *invariant.*

TH. 81 (I–XI).* Any collineation that leaves invariant an elliptic involution or a (plane) elliptic polar system is either a reflection by a pair of corresponding elements or a product of such reflections. A reflection by any pair of an elliptic involution or polar system leaves the involution or polar system invariant. By a suitably chosen transformation leaving the system invariant, any pair of incident elements of the system can be transformed into any other pair of incident elements of the same kind.

Combining results of this theorem with the theory of parallel lines (§ 6, chapter II) we are able to give a definition of congruent angles, and thus to establish the theory of similar figures. It results immediately from theorem 43 (the strong parallel proposition) that the improper projective points constitute an improper plane, whereas every other projective point is a bundle of lines, all passing through a point in the sense of chapter I. The improper plane (whose determination is unique by theorem 43) we call the plane at infinity. In this plane an elliptic polar system † Σ is arbitrarily chosen. Σ determines at every point of space a polar system of planes and lines, of which a corresponding plane and line (or pair of conjugate lines or pair of conjugate planes) are said to be mutually perpendicular. In formal terms:

DEF. 44. A plane α and line a are mutually *perpendicular* if their intersections with the plane at infinity are a pair of corresponding elements a' and A' of Σ. Two intersecting lines are perpendicular if they meet the plane at infinity in conjugate points of Σ.

DEF. 45. One angle is *congruent* to another if the sides of the one can be transformed into the sides of the other by a collineation of space that leaves Σ invariant. Since this relation is evidently mutual the angles are said to be congruent to one another.

The properties of congruent angles follow without difficulty from this definition and from theorem 81. This may be conveniently verified by comparison with HILBERT's axioms IV 4 and IV 5.

Our axioms and definitions are therefore sufficient to establish the theory of similar figures.

* There is, of course, an analogous theorem for space polar systems.

† "The imaginary circle at infinity." That the choice of Σ is arbitrary is one of the important properties of space; one tends to overlook this if congruence is introduced by axioms.

§ 8. *Congruent segments.*

To define congruent segments we have only to specify a subgroup of the group of similarity collineations of space that leave Σ (and hence, of course, the plane at infinity) invariant. A perpendicular reflection or more simply (since we shall no longer deal with other reflections) a reflection, by a proper plane α, is the reflection $(A\alpha)$ where A is the correspondent in Σ of the line a in which α meets the plane at infinity.

DEF. 46. A segment AB is *congruent* to a segment $A'B'$ if AB can be transformed into $A'B'$ by a finite number of reflections. Since this relation is evidently mutual the segments are said to be congruent to one another.

That the usual properties of congruent segments can be deduced from this definition is obvious on comparison with HILBERT's axioms IV 1, 2, 3, 6, as soon as one establishes, by the aid of thorems 79 and 80:

TH. 82 (I–XII). OA is the only segment with end-point O, in the half-line OA, that is congruent to OA.

§ 9. *The system of axioms is categorical.*

The metric properties of space having been established as indicated in § 8, the usual definitions can be given for the length of a segment in terms of a unit segment.

Coördinate axes can now be introduced in the usual way: namely, a unit of length, and three non-complanar lines through a point O are chosen arbitrarily. On each line there is thus established a correspondence between the points and the real numbers, positive and negative. The coördinates of a point P are defined as the numbers associated with the points in which three planes through the point P and parallel to the three pairs of coördinate lines meet the corresponding three coördinate lines.

TH. 83 (I–XII). To every set of three coördinates (x, y, z) corresponds a point, and to every point corresponds a set of three coördinates. The necessary and sufficient condition that three distinct points, P_1, P_2, P_3, whose coördinates are respectively $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3)$ are in the order $P_1P_2P_3$, is the existence of a number k such that $0 < k < 1$, and every one of the following fractions, not of the form $\frac{0}{0}$, is equal to k.

$$\frac{x_1 - x_2}{x_1 - x_3}, \qquad \frac{y_1 - y_2}{y_1 - y_3}, \qquad \frac{z_1 - z_2}{z_1 - z_3}.$$

TH. 84 (I–XII). If K and K' are any two classes that verify axioms I–XII, then any proposition stated in terms of points and order that is valid of the class K is valid of the class K'.

Proof. In K and in K' introduce a system of coördinates; let a point in one class correspond to a point in the other class whose coördinates are the same three numbers. By theorem 83, if three points of K are in a given order, the corresponding three points of K' are in the same order.